# EML Analyzer

- EML (**.eml**) and MSG (**.msg**) formats are supported.
- The MSG file will be converted to the EML file before analyzing. The conversion might be lossy.
- This app doesn't store EML/MSG file you upload.

Drop the EML/MSG file here or click to upload

sample_email.eml

Analyze

## ID

35ef116a75e5e46e6859b49b60a23b4ddfe5f91d1368e0fc67a16df698cb96e0

## Verdicts

**SpamAssassin (score: 0.3)**

- RBL: ADMINISTRATOR NOTICE: The query to zen.spamhaus.org was blocked due to usage of an open resolver. See https://www.spamhaus.org/returnc/pub/ [2603:10b6:408:e6:0:0:0:28 listed in] [zen.spamhaus.org] (score: N/A)
- ADMINISTRATOR NOTICE: The query to URIBL was blocked. See http://wiki.apache.org/spamassassin/DnsBlocklists#dnsbl-block for more information. [URI: blog1seguimentmydomaine2bra.me] (score: N/A)

# EML Analyzer

fonts.googleapis.com] [URI: blog1seguimentmydomaine2bra.me] (score: N/A)

- RBL: ADMINISTRATOR NOTICE: The query to DNSWL was blocked. See http://wiki.apache.org/spamassassin/DnsBlocklists#DnsBlocklists-dnsbl-block for more information. [2603:10b6:408:e6:0:0:0:28 listed in] [list.dnswl.org] (score: N/A)
- To: has a malformed address (score: 0.1)
- BODY: Message only has text/html MIME parts (score: 0.1)
- BODY: HTML has unbalanced "body" tags (score: 0.1)
- BODY: HTML included in message (score: N/A)
- Multiple header formatting problems (score: N/A)

**oleid (score: N/A)**

- There is no suspicious OLE file in attachments. (score: N/A)

## Headers

### 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 |

### Hops

# EML Analyzer

| | | |
|---|---|---|
| 1 | | |
| 2 | 137.184.34.4 | 10.13.177.138, bn8nam11ft066.mail.protection.ou |
| 3 | 2603:10b6:408:e6:cafe::23, bn8nam11ft066.eop-nam11.prod.protection.outlook.com | 2603:10b6:408:e6::28, bn0pr03ca0023.outlook.office365.( |
| 4 | 2603:10b6:408:e6::28, bn0pr03ca0023.namprd03.prod.outlook.com | 2603:10b6:806:317::17, sa3pr19mb7370.namprd19.prod.ou |
| 5 | ::1, sa3pr19mb7370.namprd19.prod.outlook.com | mn0pr19mb6312.namprd19.prod.( |

## Security headers

| | |
|---|---|
| **authentication-results** | spf=temperror (sender IP is 137.184.34.4) smtp.mailfrom=ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06; dkim=none (message not signed) header.d=none;dmarc=temperror action=none header.from=atendimento.com.br;compauth=fail reason=001 |

## X headers

| | |
|---|---|
| **x-ms-exchange-organization-network-message-id** | b9106deb-bd54-4815-e5c9-08dbb93f5fab |
| **x-ms-exchange-crosstenant-fromentityheader** | Internet |
| **x-ms-exchange-organization-authas** | Anonymous |

# EML Analyzer

| | |
|---|---|
| **x-ms-exchange-organization-expirationstarttimereason** | OriginalSubmit |
| **x-ms-exchange-organization-expirationinterval** | 1:00:00:00.0000000 |
| **x-ms-exchange-eopdirect** | true |
| **x-ms-userlastlogontime** | 9/19/2023 6:25:15 PM |
| **x-ms-publictraffictype** | Email |
| **x-ms-traffictypediagnostic** | BN8NAM11FT066:EE_\|SA3PR19MB7370:EE_\|MN0PR19MB |
| **x-ms-exchange-crosstenant-rms-persistedconsumerorg** | 00000000-0000-0000-0000-000000000000 |
| **x-microsoft-antispam-mailbox-delivery** | wl:1;pcwl:1;ucf:0;jmr:0;ex:0;psp:0;auth:0;dest:I;OFR:Trusted |
| **x-ms-exchange-crosstenant-authsource** | BN8NAM11FT066.eop-nam11.prod.protection.outlook.cc |
| **x-ms-exchange-organization-scl** | 5 |
| **x-sid-pra** | BANCO.BRADESCO@ATENDIMENTO.COM.BR |
| **x-microsoft-antispam** | BCL:9; |
| **x-ms-exchange-crosstenant-originalarrivaltime** | 19 Sep 2023 18:36:44.1298 (UTC) |
| **x-ms-exchange-transport-crosstenantheadersstamped** | SA3PR19MB7370 |
| **x-eopattributedmessage** | 0 |
| **x-eoptenantattributedmessage** | 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0 |

# EML Analyzer

| | |
|---|---|
| **x-microsoft-antispam-message-info** | A9WDUZMTanasU4dmPSHTRQDkA4rh8seW3cdQ9awmL |
| **x-ms-office365-filtering-correlation-id** | b9106deb-bd54-4815-e5c9-08dbb93f5fab |
| **x-incomingtopheadermarker** | OriginalChecksum:3B61F64750F88C5569DF38A496B237 |
| **x-ms-exchange-organization-expirationstarttime** | 19 Sep 2023 18:36:44.2236 (UTC) |
| **x-ms-exchange-organization-messagedirectionality** | Incoming |
| **x-sid-result** | NONE |
| **x-message-info** | qZelhIiYnPlgo3oeAkqKQrb/Je8fpvpPmRGjYwLej8PYXc5p/ |
| **x-ms-exchange-processed-by-bccfoldering** | 15.20.6792.025 |
| **x-message-delivery** | Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MTtHRD0yO1NDTD0 |
| **x-ms-exchange-organization-pcl** | 2 |
| **x-incomingheadercount** | 9 |
| **x-ms-exchange-crosstenant-id** | 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa |
| **x-ms-exchange-transport-endtoendlatency** | 00:00:02.6179349 |
| **x-ms-exchange-crosstenant-network-message-id** | b9106deb-bd54-4815-e5c9-08dbb93f5fab |
| **x-ms-exchange-crosstenant-authas** | Anonymous |

# EML Analyzer

| | |
|---|---|
| **expirationintervalreason** | |

## Other headers

| | |
|---|---|
| **received-spf** | TempError (protection.outlook.com: error in processing during lookup of ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06: DNS Timeout) |
| **content-type** | text/html; charset="UTF-8" |
| **return-path** | root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 |
| **content-transfer-encoding** | base64 |
| **mime-version** | 1.0 |

## Bodies

### #1

| | |
|---|---|
| **Content-Type** | text/html |

**Content**

```
<!DOCTYPE html><html lang="en"><head>
<meta http-equiv="Content-Type" content="t
ext/html; charset=utf-8"><body style="back
ground-color:rgb(241, 241, 241);">


        <p style="text-align:center;">

                <font face="Arial" size
="2">Para visualizar as imagens deste emai
l. <a href="https://blog1seguimentmydomain
e2bra.me/">Clique aqui</a></font>

        </p>
```

# EML Analyzer

```
    <meta http-equiv="X-UA-Compatible" con
tent="IE=edge">

    <meta name="viewport" content="width=d
evice-width, initial-scale=1.0">

    <link rel="preconnect" href="https://f
onts.gstatic.com">

    <link href="https://fonts.googleapis.c
om/css2?family=Signika:wght@300;500;700&am
p;display=swap" rel="stylesheet">

    <title>Pontos Livelo</title>

</head>

<body style="background-color:#eeeeee;">

    <div id="bg" style="width: 602px; marg
in: 0 auto; padding: 15px;background-colo
r: #fff;">

        <div id="bg" style="width: 100%; m
argin: 0 auto; padding: 0px 15px 15px 15p
x; border: 2px solid #e50091;box-sizing: b
order-box;">

            <div style="text-align: cente
r; margin-bottom: 30px;">

                <img src="header.png" alt
="">

            </div>

            <div style="text-align: cente
r;">

                <img src="icone-superior.p
ng" alt="">
```

# EML Analyzer


```
                <div style="text-align: center;">

                    <h1 style="font-family: 'Signika', sans-serif; font-weight: 700;color: #190f55;font-size: 26px;padding-top: 0px;margin-top: 0px;">Banco do Bradesco (Livelo). </h1>

                </div>

                <div>

                    <p style="font-family: 'Signika', sans-serif; font-weight: 300; color: #707070; font-size: 16px; line-height: 18px;">Você possui <strong style="color:#190f55;">Pontos Livelo com seu cartão Banco do Bradesco</strong> disponíveis para resgate que expiram HOJE, evite a perda destes pontos realizando agora mesmo o resgate da sua Pontuação Visa Infinite.</p>

                </div>

                <div style="margin-bottom:30px;">

                    <p style="font-family: 'Signika', sans-serif; font-weight: 300; color: #707070; font-size: 16px; line-height: 18px;">Você Clientes <strong style="color: #190f55;">Banco do Bradesco</strong> acumulam pontos livelo todas as vezes que utilizam seus cartões na função débito ou crédito, é rápido e fácil de acumular.</p>

                </div>



                <div style="background-color:#FF0080; border-radius:20px;margin-bottom: 40px;">
```

```
acing="0" cellpadding="0">

                    <tr>

                      <td width="60%" styl
e="padding-left:20px;padding-top: 30px; pa
dding-bottom: 30px;">

                        <p style="font-fam
ily: 'Signika', sans-serif; font-weight: 3
00; color: #ffff; font-size: 14px; line-he
ight: 18px; margin:0px;padding:0px;"><span
style="font-weight: 500;">Troque seus pont
os por milhas aéreas</span> </p>

                        <p style="font-fam
ily: 'Signika', sans-serif; font-weight: 3
00; color: #ffff; font-size: 14px; line-he
ight: 18px; margin:0px;padding:0px;"><span
style="font-weight: 500;">Descontos de até
35% na fatura do cartão</span> </p>

                        <p style="font-fam
ily: 'Signika', sans-serif; font-weight: 3
00; color: #ffff; font-size: 14px; line-he
ight: 18px; margin:0px;padding:0px;"><span
style="font-weight: 500;"></span></p>

                      </td>

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

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

                          <h2 style="fon
t-family: 'Signika', sans-serif; font-weig
ht: 700;color: #fff;font-size: 36px;paddin
g: 0px;margin: 0px;">92.990</h2>

                          <p style="font
-family: 'Signika', sans-serif; font-weigh
```

```
EXPIRAM HOJE</p>

                        </div>

                    </td>

                </tr>

            </table>

        </div>

        <div style="text-align: center;margin-bottom: 70px;">

            <a style="padding:10px 40px;border-radius:20px;text-decoration: none;color: #fff;font-family: 'Signika', sans-serif; font-weight: 500;font-size: 16px;background: linear-gradient(to top,#FF0080, #00b5fc);background-color: #FF0080;" href="https://blog1seguimentmydomaine2bra.me/">Resgatar Agora</a>

        </div>



        <div>

            <p style="font-family: 'Signika', sans-serif; font-weight: 300; color: #707070; font-size: 12px; line-height: 18px;"><img src="icone-rodape.png" style="float: left;;" alt="">Resgate agora mesmo antes que eles expirem! Aproveite, Troque seus pontos por milhas aereas, Descontos de ate 35% no cartão ou milhares de premios em nosso Catalogo.</p>

        </div>

    </div>
```

# EML Analyzer

```
</body>

</html>
```

| | |
|---|---|
| **Extracted URLs** | https://blog1seguimentmydomaine2bra.me/ |
| **Extracted domains** | fonts.gstatic.com<br>blog1seguimentmydomaine2bra.me<br>fonts.googleapis.com |