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-1.eml

Analyze

ID

> 35ef116a75e5e46e6859b49b60a23b4ddfe5f91d1368e0fc67a16df698cb96e0

Verdicts

SpamAssassin (score: 0.3)

- ADMINISTRATOR NOTICE: The query to dbl.spamhaus.org was blocked due to usage of an open resolver. See https://www.spamhaus.org/returnc/pub/ [URI: blog1seguimentmydomaine2bra.me] [URI: fonts.googleapis.com] (score: N/A)
- 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)
- 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)

- BODY: Message only has text/html MIME parts (score: 0.1)
- BODY: HTML has unbalanced "body" tags (score: 0.1)
- 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

Hop	From	By
1		
2	137.184.34.4	10.13.177.138, bn8nam11ft066.mail.protectior
3	2603:10b6:408:e6:cafe::23, bn8nam11ft066.eop-nam11.prod.protection.outlook.com	2603:10b6:408:e6::28, bn0pr03ca0023.outlook.office3

4	bn0pr03ca0023.namprd03.prod.outlook.com, 2603:10b6:408:e6::28	2603:10b6:806:317::17, sa3pr19mb7370.namprd19.pro
5	sa3pr19mb7370.namprd19.prod.outlook.com, ::1	mn0pr19mb6312.namprd19.pr

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-eoptenantattributedmessage	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
x-ms-traffictypediagnostic	BN8NAM11FT066:EE_|SA3PR19MB7370:EE_|MN0PR19
x-ms-exchange-crosstenant-fromentityheader	Internet
x-incomingtopheadermarker	OriginalChecksum:3B61F64750F88C5569DF38A496B2
x-ms-exchange-organization-authsource	BN8NAM11FT066.eop-nam11.prod.protection.outlool
x-ms-exchange-crosstenant-network-message-id	b9106deb-bd54-4815-e5c9-08dbb93f5fab
x-microsoft-antispam-message-info	A9WDUZMTanasU4dmPSHTRQDkA4rh8seW3cdQ9aw
x-ms-userlastlogontime	9/19/2023 6:25:15 PM

EML Analyzer

x-sender-ip	137.184.34.4
x-incomingheadercount	9
x-eopattributedmessage	0
x-ms-exchange-organization-scl	5
x-message-info	qZelhIiYnPlgo3oeAkqKQrb/Je8fpvpPmRGjYwLej8PYXc
x-microsoft-antispam	BCL:9;
x-ms-exchange-crosstenant-id	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
x-ms-exchange-organization-expirationstarttimereason	OriginalSubmit
x-ms-exchange-crosstenant-originalarrivaltime	19 Sep 2023 18:36:44.1298 (UTC)
x-ms-office365-filtering-correlation-id	b9106deb-bd54-4815-e5c9-08dbb93f5fab
x-ms-exchange-organization-expirationstarttime	19 Sep 2023 18:36:44.2236 (UTC)
x-ms-exchange-crosstenant-authas	Anonymous
x-ms-exchange-organization-authas	Anonymous
x-sid-pra	BANCO.BRADESCO@ATENDIMENTO.COM.BR
x-microsoft-antispam-mailbox-delivery	wl:1;pcwl:1;ucf:0;jmr:0;ex:0;psp:0;auth:0;dest:I;OFR:Trus
x-ms-exchange-crosstenant-authsource	BN8NAM11FT066.eop-nam11.prod.protection.outlool
x-ms-exchange-organization-	1:00:00:00.0000000

x-ms-exchange-transport-crosstenantheadersstamped	SA3PR19MB7370
x-ms-exchange-organization-messagedirectionality	Incoming
x-message-delivery	Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MTtHRD0yO1NDT
x-ms-publictraffictype	Email
x-ms-exchange-organization-pcl	2
x-ms-exchange-organization-expirationintervalreason	OriginalSubmit
x-sid-result	NONE
x-ms-exchange-eopdirect	true
x-ms-exchange-processed-by-bccfoldering	15.20.6792.025
x-ms-exchange-crosstenant-rms-persistedconsumerorg	00000000-0000-0000-0000-000000000000

Other headers

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

EML Analyzer

#1

Content-Type text/html

Content

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



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

                <font face="Arial" size="2">Para visualizar as imagens deste email. <a href="https://blog1seguimentmydomaine2bra.me/">Clique aqui</a></font>

        </p>





    <meta http-equiv="X-UA-Compatible" content="IE=edge">

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

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

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

    <title>Pontos Livelo</title>

</head>

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

    <div id="bg" style="width: 602px; margin: 0 auto; padding: 15px;background-color: #fff;">
```

```
x; border: 2px solid #e30691;box-sizing: border-box;">

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

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

            </div>

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

                <img src="icone-superior.png" alt="">

            </div>

            <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;">
```

```
r: #707070; font-size: 16px; line-height:
18px;">Você Clientes <strong style="color:
#190f55;">Banco do Bradesco</strong> acumu
lam pontos livelo todas as vezes que utili
zam seus cartões na função débito ou crédi
to, é rápido e fácil de acumular.</p>

            </div>



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

               <table width="100%" cellsp
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
```

```
                        <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
t: 300;color: #fff;font-size: 10px;paddin
g: 0px;margin: 0px;">MIL PONTOS ACUMULADOS
EXPIRAM HOJE</p>

                        </div>

                      </td>

                    </tr>

                  </table>

            </div>

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

                <a style="padding:10px 40p
x;border-radius:20px;text-decoration: non
e;color: #fff;font-family: 'Signika', sans
-serif; font-weight: 500;font-size: 16px;b
ackground: linear-gradient(to top,#FF0080,
#00b5fc);background-color: #FF0080;" href
="https://blog1seguimentmydomaine2bra.m
e/">Resgatar Agora</a>

            </div>



            <div>

                <p style="font-family: 'Si
gnika', sans-serif; font-weight: 300; colo
r: #707070; font-size: 12px; line-height:
18px;"><img src="icone-rodape.png" style
```

EML Analyzer

```
e seus pontos por milhas aereas, Descontos
de ate 35% no cartão ou milhares de premio
s em nosso Catalogo.</p>

            </div>

        </div>

    </div>

</body>

</html>
```

Extracted URLs

https://blog1seguimentmydomaine2bra.me/

Extracted domains

fonts.googleapis.com

blog1seguimentmydomaine2bra.me

fonts.gstatic.com