Phishing Analysis Report - 001

Case Number: 001
Report By: Rishab Hamesh Shorey
Documented on: 11/11/2025
File Name: Sample-1.eml
File Link: https://github.com/rf-peixoto/phishing_pot/blob/main/email/sample-1.eml

Headers

==========
Language: Portuguese (Brazil)
Date of Email: September 12, 2025

To: phishing@pot
From: banco.bradesco@atendimento.com.br

Subject Line:
CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!

Return-Path:
root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06

Sender IP:
137.184.34.4
Resolve Host:

Message-ID:
<20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06>

URLs

==========
Fanged URL:
hxxps[://]blog1seguimentmydomaine2bra[.]me/

Attachments

==========
Attachment Name: N/A
Attachment Link:

MD5:
N/A
SHA1:
N/A
SHA256:
N/A

Description

==========

We are able to see that the attacker over here is trying to imitate someone, specially seen: **Banco do Bradesco** (**Livelo**). This is a bank in Brazil who they are trying to imitate.

According to the translated message the attacker is asking the user to redeem the points for the credit card in either **debit or credit mode**. There is a sense of urgency which is created over here and trying to trick the user into clicking a link to redirect them into another site of a blog as per analysis.

There are several kind of IOC which is attempting to temp the user to redeem its points as it portrays that the expiration happens today.

Tools Used For Analysis

==========

1. Virus Total
2. WannaBrowse
3. Paloaltonetwork
4. URL Void
5. CheckPhish
6. URL2PNG
7. ThreatCop

Artifact Analysis

==========

Sender Analysis:
The user is claiming to be from bank of Bradesco but the domain does not seem to be from the originating source, it is using different domain, that does not have any kind of relation with the **Banco de Bradesco** but smartly speaking the correct TLD is being used.

Usually credit points do not get expired and discount prices gets retained so it is highly suspected that the sender is trying to fixate a sense of an urgency here.

URL Analysis:
After conducting URL analysis of with various tools we do not get any result as such. The URL does not redirect to the original bank site or any of its subdomain. The URL is in its original form.

There is no screenshot available for it, there is no location or IP address that this site redirects to. It means that there is no kind of server or domain as such that exist with regards to this link.

Even though upon clicking there isn't any kind of activity taken place. The site is showing unreachable, so we cannot confirm any kind of weird activity taken place at-least from the first view naked eye.

Images of Site:

Attachment Analysis:
N/A

Attachment Preview:

Verdict

==========

Considering that domain does not even come close to matching with the body of the Email i.e. Bank of Bradesco and some Blog Page mentioned.

- It clear that the mail could be used either to gather information to see if the sender's domain is legitimate or no.
- There could be tagged parameters within the link itself which indicates that the receiver has seen the message or no
- There is also no security parameters enabled for the Email which makes it highly doubtful.

My final verdict concludes saying that a low risk level, it is probable that it is some kind of clickbait.

Defense Actions

==========

Considering it can be a user from the enterprise level who is targeted hence:

Containment & **Eradication**- Would ensure to block certain link from the reaching our server, specially with certain headline. Most possibly that the users are having an account in Bank of Bradesco hence with certain subject lines and domains shall be prevented.

No Recovery needed at the moment.

Communication: The official communication can be made that no promotion or any bank related activity shall be sent to the account of the users, all official salary crediting notification shall be done via the company portal for employees itself at their dashboard.