Report: Analysis of "BRADESCO LIVELO" Phishing Email

Date: October 27, 2025
Analyst: (KONATHAM SAI RAM CHANDU)
Artifacts: `BRADESCO LIVELO.eml`, `Header-Analysis.pdf`

Summary:
The email sample was analyzed and confirmed to be a **phishing attack**. The goal is **credential harvesting**. The email uses social engineering (extreme urgency) to scare the user into "redeeming" expiring points. The malicious link is designed to take the user to a fake website that mimics the real Bradesco or Livelo portal, where their bank login and password would be stolen.

Phishing Indicators Found:

1. **Social Engineering (Urgency):**
  * [cite_start]**Finding:** The subject line is `CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!` (Your card has 92,990 LIVELO points expiring today!). [cite: 9, 358]
  * **Analysis:** This is a high-pressure tactic. By giving a large point value and a 24-hour deadline ("expirando hoje"), the attacker creates panic, forcing the user to act quickly without scrutinizing the email.

2. **Suspicious Sender Domain (Spoofing):**
  * [cite_start]**Finding:** The `From:` address is `BANCO DO BRADESCO LIVELO<banco.bradesco@atendimento.com.br>`. [cite: 94, 185, 358]
  * **Analysis:** This is designed to look legitimate, but the actual domain is `atendimento.com.br`. This is a generic domain (meaning "support" in Portuguese) and is **not** the official bank domain (`bradesco.com.br`).

3. **Failed Email Authentication (Technical Proof):**
  * **Finding:** The header analysis shows critical authentication failures.
    * [cite_start]`dkim=none (message not signed)`. [cite: 88, 175, 355] [cite_start]The MxToolbox report confirms: `No DKIM-Signature header found`. [cite: 69]
    * [cite_start]`compauth=fail reason=001`. [cite: 88, 176, 355] This is Microsoft's "Composite Authentication," and it explicitly **failed**, indicating it's a spoofed email.
  * **Analysis:** Legitimate banks *always* use DKIM to sign their emails as proof of identity. The lack of a DKIM signature and the `compauth=fail` are definitive proof this email is fraudulent.

4. **Suspicious Origin Server & Return Path:**
  * [cite_start]**Finding:** The email originated from a server named `ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06` [cite: 26, 178, 356] [cite_start]at IP address

`137.184.34.4`. [cite: 139, 178, 215, 356] [cite_start]The `Return-Path` (where bounce-backs go) is `root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06`. [cite: 113, 190]
    * **Analysis:** This server name indicates a generic, disposable cloud virtual machine (like from DigitalOcean or Vultr). A multi-billion dollar bank would *never* send security alerts from a generic server's `root` user.

5. **Malicious Destination Link:**
    * [cite_start]**Finding:** The Base64-encoded HTML body [cite: 264, 343] contains the call-to-action link "Resgatar Agora" (Redeem Now).
    * **Analysis:** Decoding the Base64 reveals the link's true destination: `https://blog1seguimentmydomaine2bra.me/`. This domain is unrelated to Bradesco or Livelo and is clearly a suspicious, attacker-controlled site.

6. **High Spam & Bulk Complaint Scores:**
    * **Finding:** The email was flagged by Microsoft's filters before it even reached the inbox.
        * [cite_start]`X-MS-Exchange-Organization-SCL: 5` (Spam Confidence Level 5 = Spam) [cite: 139, 220]
        * [cite_start]`X-Microsoft-Antispam: BCL:9;` (Bulk Complaint Level 9 = High) [cite: 139, 221]
    * **Analysis:** This shows that the sending IP/domain has a very bad reputation and many other users have already marked these emails as spam.