### **Introduction**

This report summarizes the findings from an analysis of a suspected phishing email, using the sample.eml file and extracted metadata through email header and body inspection tools.

### **Email Overview**

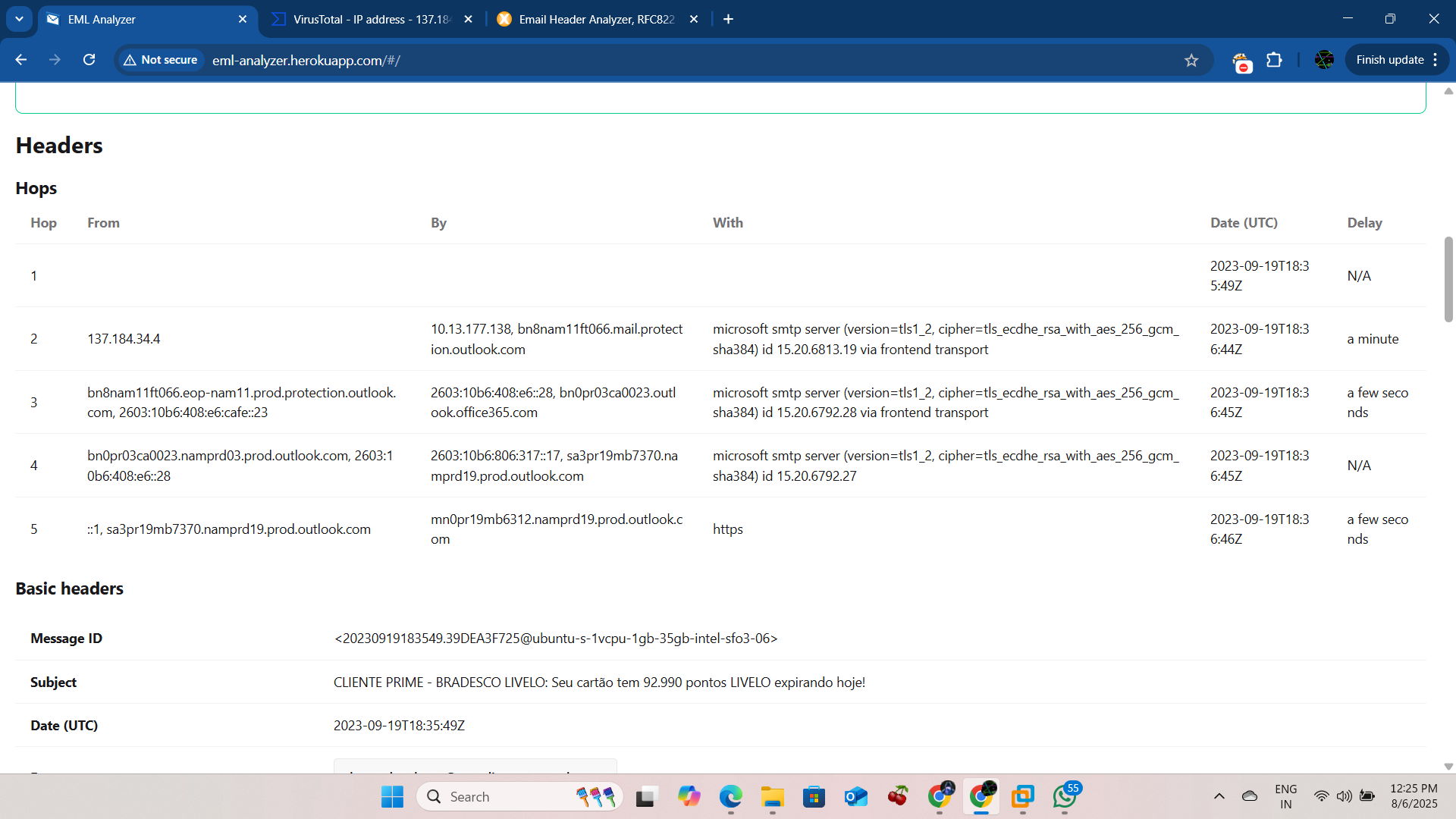
* **Subject**: CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!
* **Sender**: [banco.bradesco@atendimento.com.br](mailto:banco.bradesco@atendimento.com.br)
* **Return Path**: root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
* **IP Address**: 137.184.34.4 (Hosted on DigitalOcean VPS)
* **Date**: 2023-09-19 18:35:49 UTC

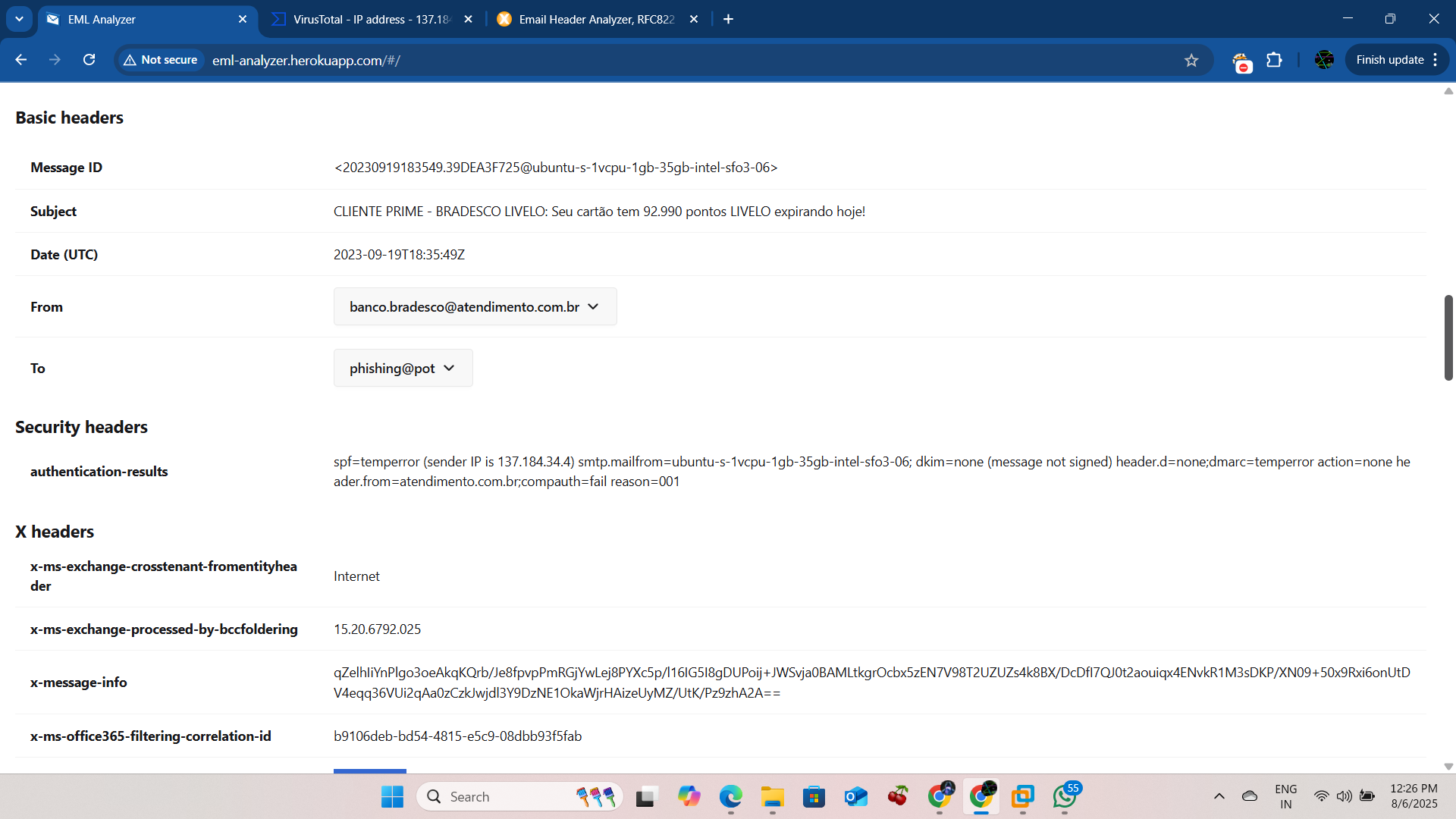
### **Phishing Traits Identified**

1. **Spoofed Sender Address**: The email pretends to be from Bradesco Bank but uses the fake domain atendimento.com.br.
2. **Urgent Language**: Creates pressure by stating that points will “expire today”.
3. **Return Path Discrepancy**: The return path is from a server with a generic VPS hostname, not from a legitimate financial institution.
4. **Authentication Failures**:
   1. SPF: temperror
   2. DKIM: none (not signed)
   3. DMARC: temperror
   4. compauth=fail
   5. compauth=fail
5. **Malicious URL**: Contains a suspicious phishing link:  
    <https://blog1seguimentmydomaine2bra.me/>
6. **Suspicious Origin IP**: The message was sent from 137.184.34.4 – a VPS address unrelated to Bradesco.
7. **Poor Message Quality**: Low-quality design, formatting, and fake urgency typical of mass phishing campaigns.

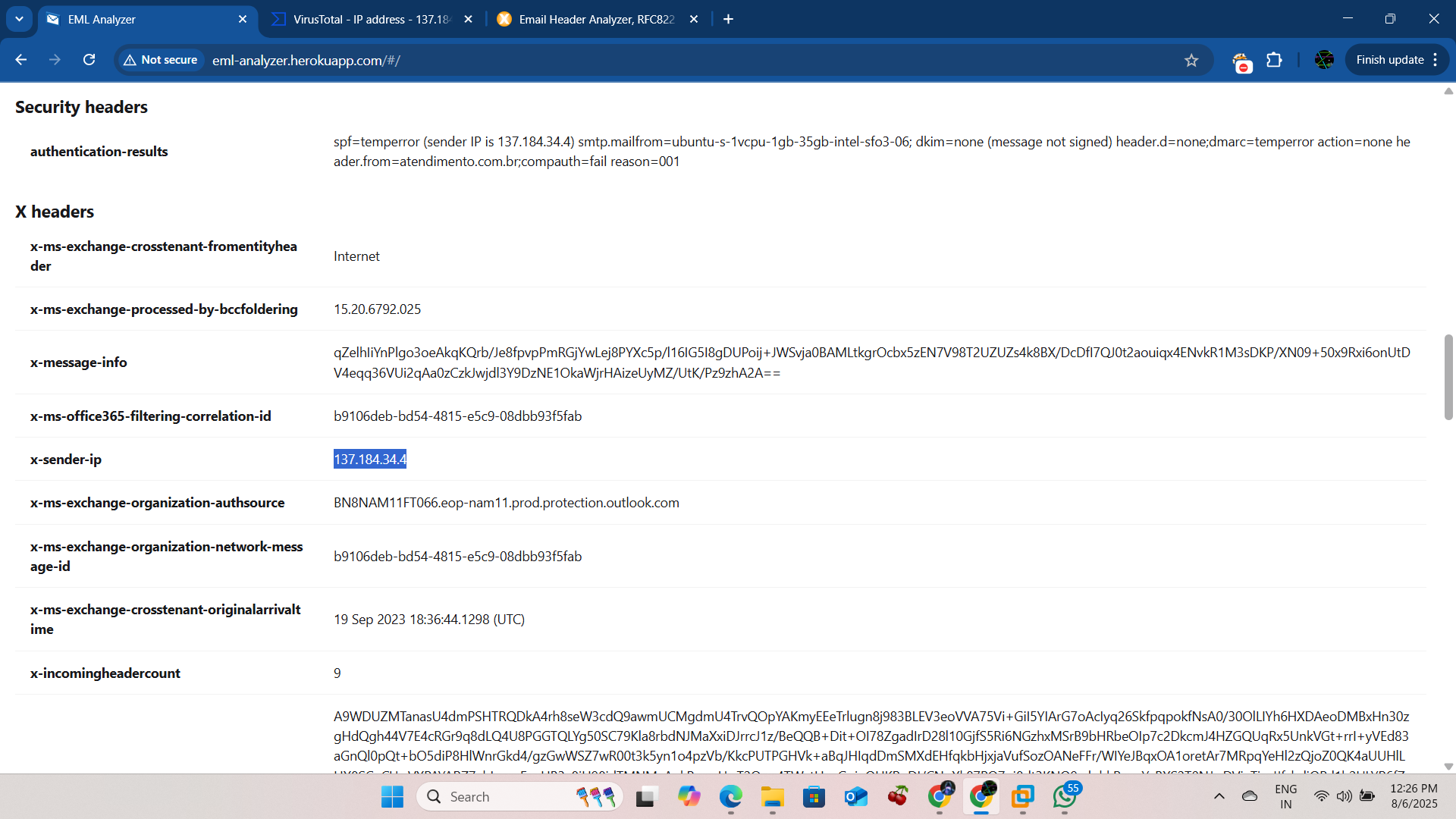
Evidence (Screenshots)

Header hops and metadata





SPF, DKIM, DMARC authentication failures



### **Conclusion**

The analyzed email displays multiple clear indicators of a phishing attempt. It uses social engineering tactics, fails standard authentication mechanisms, originates from a suspicious VPS, and includes a phishing link targeting user credentials. It is advised to avoid clicking any links and report this email as phishing.