Executive Summary
==

This report analyzes a phishing email impersonating Bradesco bank, sent from an unrelated email address. The attacker attempts to trick the recipient into clicking a fraudulent link under the pretext of getting Livelo points before they expire. Indicators of compromise include urgency tactics, failure of DKIM authentication, the use of a malicious Webflow-hosted URL, and the use of a non-legitimate email address. Although the phishing page has since been removed, the email demonstrates typical characteristics of credential-harvesting attempts. Defensive actions were taken to block the sender and associated domains to prevent further exposure.

Headers
==

Date: Tue, 19 Sep 2023 18:35:49 +0000 (UTC)
Subject: CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!

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

Reply-To: None
Return-Path: root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06

Sender IP: 137.184.34.4
Resolve Host: buntu-s-1vcpu-1gb-35gb-intel-sfo3-06

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

URLs
==

hxxps[://]blog1seguimentmydomaine2bra[.]me/

Description
==

The email is in Brazilian and claims to be from Bradesco bank. It claims the receiver has Livelo Points available for redemption that expire today if not redeemed immediately. There is a prominent Redeem Now button in the email.

Bradesco bank is a major private-sector financial and insurance services provider in Brazil, offering a wide range of banking products and insurance services to individuals, businesses, and corporations.

Livelo points are units of a large loyalty and rewards program in Brazil, where users earn points through purchases with partner companies, participating credit cards, and the Livelo platform.

There are several indicators of urgency: It mentions several times how the points will expire today, and how easy it is to just redeem them.

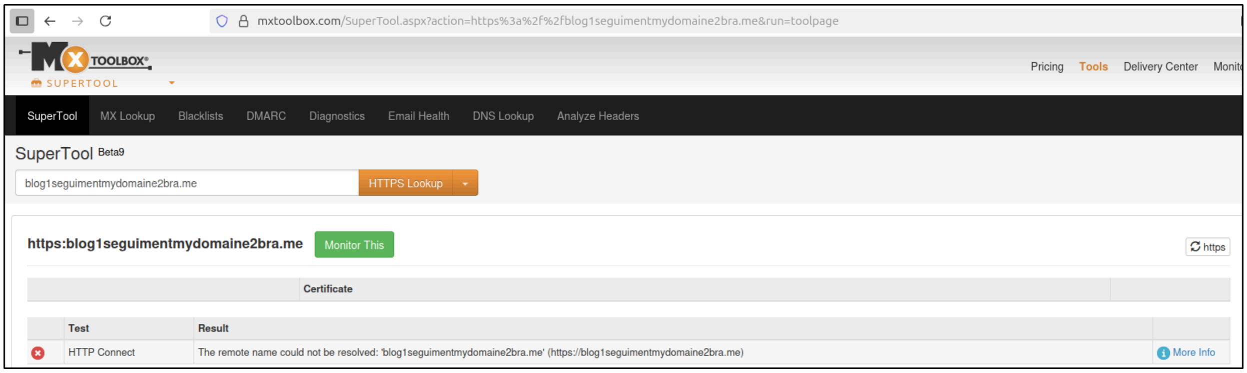
Artifact Analysis
==
Sender Analysis:
The sender's From email address domain is not related to the Bradesco bank or Livelo. The domain name translates to something general like 'service'.

The Return-Path and Received header show a name "ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06" which may be the attacker's host. The IP address is related to a cloud service called Digital Ocean.

URL Analysis:
The URL is not related to either Bradesco bank or Livelo, and seems to just have been a temporary website for this phish. It is no longer available: any DNS lookups give a Domain Not Found error.

Verdict
==
Due to the sender not being affiliated with either Bradesco bank or Livelo, this is a clear impersonation and spoofing attempt.

Additionally, the URL is also not related to these companies and the website is no longer available.



SuperTool Beta9

blog1seguimentmydomaine2bra.me

https:blog1seguimentmydomaine2bra.me

Certificate

	Test	Result	
☒	HTTP Connect	The remote name could not be resolved: 'blog1seguimentmydomaine2bra.me' (https://blog1seguimentmydomaine2bra.me)	More Info

Any sandboxing attempts therefore failed. However, legitimate services would not use a temporary alternate website to redeem points.

As a result of the analysis, this email has been determined to be malicious.

Defense Actions
=======================================

After performing a message trace, no other users within the organization received an email from this sender or with a similar subject line.

To prevent the malicious sender from sending any other email to the organization, I have blocked the “banco.bradesco@atendimento.com.br“ email address on the email gateway. The atendimento[.]com[.]br domain does not seem to be related to any actual legitimate companies or services.

To ensure users are unable to access this malicious URL or domain, I have blocked “blog1seguimentmydomaine2bra[.]me” on the EDR and on the Web Proxy. While the website seems to have been removed, it is unlikely that a legitimate service will use that domain in the future.