Email samples and screenshots in this analysis are from Phishing Pot by Peixoto, licensed under CC BY-NC 4.0. The original sample analysed in this report can be found below:

Phishing Pot: https://github.com/rf-peixoto/phishing_pot
Peixoto: https://github.com/rf-peixoto
License: https://github.com/rf-peixoto/phishing_pot/blob/main/LICENSE
Source file: https://github.com/rf-peixoto/phishing_pot/blob/main/email/sample-1844.eml

Executive Summary
==========
This report analyzes a phishing email impersonating Nubank, sent from a free Gmail address. The attacker attempts to trick the recipient into clicking a fraudulent link in a pdf attachment by claiming not doing so will result in a potentially fraudulent bank transfer. Indicators of compromise include urgency tactics, grammar issues, malicious file hash, and the use of malicious URLs. The email demonstrates typical characteristics of malware propagation attempts. Defensive actions were taken to block the sender and associated domains to prevent further exposure.

Headers
==========
Date: Wed, 08 Nov 2023 08:39:10 -0800 (PST)
Subject: Valor bloqueado por segurancaNm9ehEyNWyox3

To: phish@pot
From: Nubank - suspeita de fraudeqoLEDh3Qm2 <plop77646@gmail.com>

Reply-To: None
Return-Path: plop77646@gmail.com

Sender IP: 51.222.185.233 (OVH, Canada)
Resolve Host: ip233.ip-51-222-185.net

Message-ID: <654bb9ae.c80a0220.5e3eb.5137@mx.google.com>

Attachments
==========
Attachment Name: pdf_YJur9usLK2.pdf
MD5: f595c168f07216de0f983c2de72a3103
SHA1: cbbf3f93cb453a3f4a1a68f000540fa977d67a56
SHA256: dff27b41956682052d1096eda02282bb2d96f7049244dfea16a9ee7fe56e1d3a

URLs

==========
hxxps[://]acessoseguro[.]blob[.]core[.]windows[.]net/acesso2023/382718256cd5a8d0[.]html

Description
==========
It is an email in Brazilian Portuguese, claiming to be from Nubank. It says that a transfer was suspended due to suspected fraud. It says that there is a transfer pending worth over four thousand Brazilian Real, and that they only have 24 hours to dispute the charge. For more information, the user needs to view a pdf file that is attached to the email.

There are several indicators of urgency: The user needs to dispute the charge within 24 hours, or else lose over four thousand Reals.

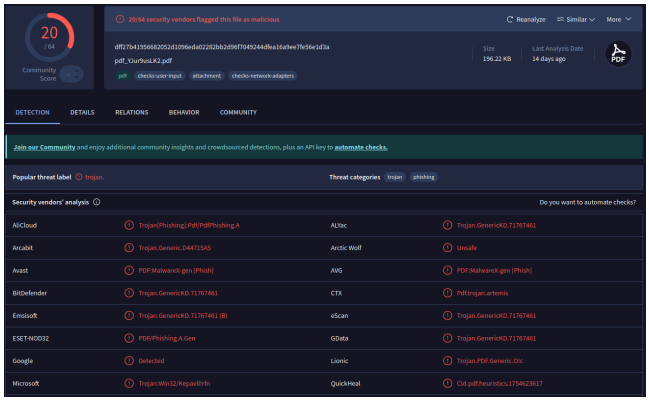
The message contains multiple linguistic anomalies: CPF is a tax number, and should not have an email address filled in. A number of words miss accents (a instead of ã) or cedillas (c instead of ç)

It also mentions personal information such as the name and half the CPF number of the supposed recipient, which is unusual.

Artifact Analysis
==========
Sender Analysis:
The email claims to be from Nubank, but the email used is Gmail. This is obfuscated with the display name being “Nubank - suspeita de fraudeqoLEDh3Qm2”.

The sender IP resolves to OVH, a legitimate hosting provider frequently abused by attackers for disposable VPS infrastructure.

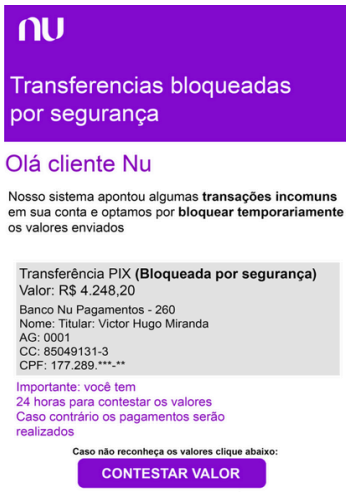
Attachment Analysis:
The attachment’s hash values can be looked up on VirusTotal, where 20 security vendors say it is malicious, specifically a Trojan.

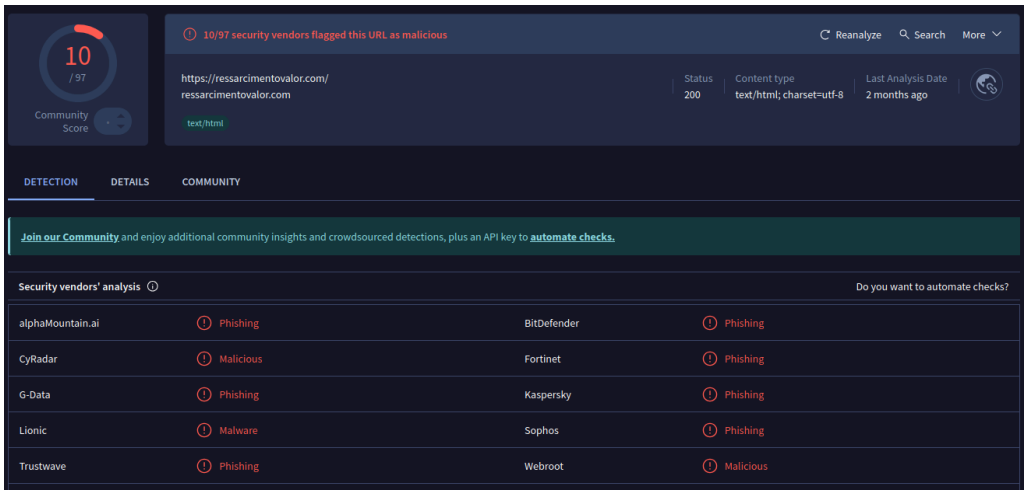


Dumping the file and then running it in Hybrid Analysis' sandboxing service, it shows that the document repeats the information in the email, and asks the user to click on a URL:

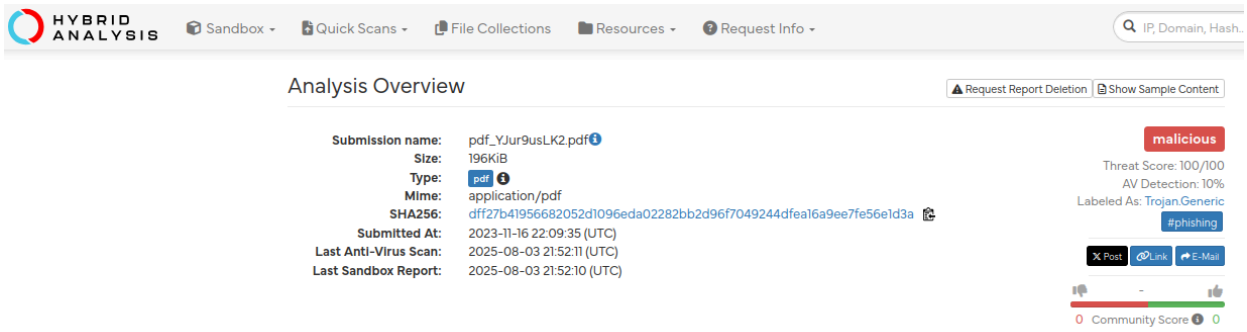
hxxps[://]acessoseguro[.]blob[.]core[.]windows[.]net/acesso2023/382718256cd5a8d0[.]html

This URL redirects to **hxxps[://]ressarcimentovalor[.]com**. On VirusTotal, 20 security vendors say the URL is malicious.





Additionally, the Hybrid Analysis sandbox reports also give the file a malicious rating and calls it a Trojan:



Verdict
==========
Due to the sender claiming to be a bank even though they are using a generic Gmail address, this is a clear impersonation and spoofing attempt. A service like a Bank would use their own email domain and would also not make the linguistic mistakes that can be seen in the email.

Additionally, the file attachment tries to trick the user into clicking a malicious URL. Both the file and link have been deemed malicious by VirusTotal and Hybrid Analysis.

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 “plop77646@gmail[.]com” email and the file’s hashes on the email gateway.

To ensure users are unable to access these malicious URLs or domains, I have blocked the below URL and domain on the EDR and on the Web Proxy.
acessoseguro[.]blob[.]core[.]windows[.]net/acesso2023/382718256cd5a8d0[.]html
Ressarcimentovalor[.]com