Phishing Analysis Report

Summary:

Phishing email targeting a user named C*YNTHIA TIEMI SUZUKI. Contains multiple Trojans.*

Description:

The suspicious email was crafted in Portuguese, targeting a user named *"CYNTHIA TIEMI SUZUKI."* The message informed the recipient that their account had been blocked and urged them to open an attached file for further information. It also contained a "release code" (`86258767265340165`), used as a social engineering tactic to add legitimacy and urgency.

Upon inspection, the attached PDF was found to be malicious. Analysis revealed that it contained multiple embedded Trojans and three additional `.dat` files, all of which were confirmed as malware payloads. The file is designed to deliver a phishing Trojan, which attempts to steal sensitive user data and potentially establish persistence on the victim system.

The combination of urgency, attachment-based payload delivery, and the presence of multiple malicious artifacts strongly indicates that this email is a phishing campaign aimed at credential theft and further compromise.

Header Analysis:

Date: Thu, 17 Aug 2023 18:35:25 +0000

Subject: Ourocard - Liberacao.VXfQMHkaoGC4YFK4kX1

To: <phishing@pot>

From: marthacartersddqym@gmail.com

Return-Path: marthacartersddqym@gmail.com

Sender IP: 209.85.215.182

Resolve Host: mail-pg1-f182.google.com

Message-ID: <a149b78f3ae0393de0a46c4d14eb79a2@gmail.com>

Email Content Analysis:

Language: Written in Portuguese.

Translation: "CLIENT: CYNTHIA TIEMI SUZUKI

We have blocked your account

More information in the attachment.

Release code: 86258767265340165"

Tone: Urgency + fear. ("We blocked your account") --common phishing technique to scare the user into acting quickly.

Call-to-Action: Attacker wants user to open the sent attachment and enter the “Release Code”.

Authentication Results:

SPF: pass (sender IP is 209.85.215.182) smtp.mailfrom=gmail.com

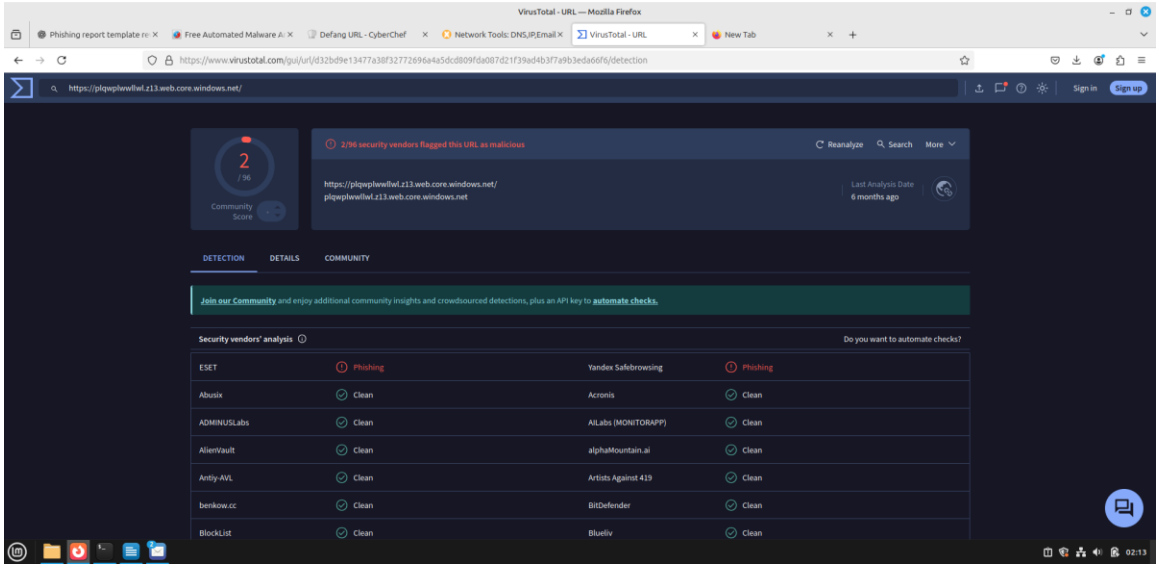
DKIM: pass (signature was verified) header.d=gmail.com

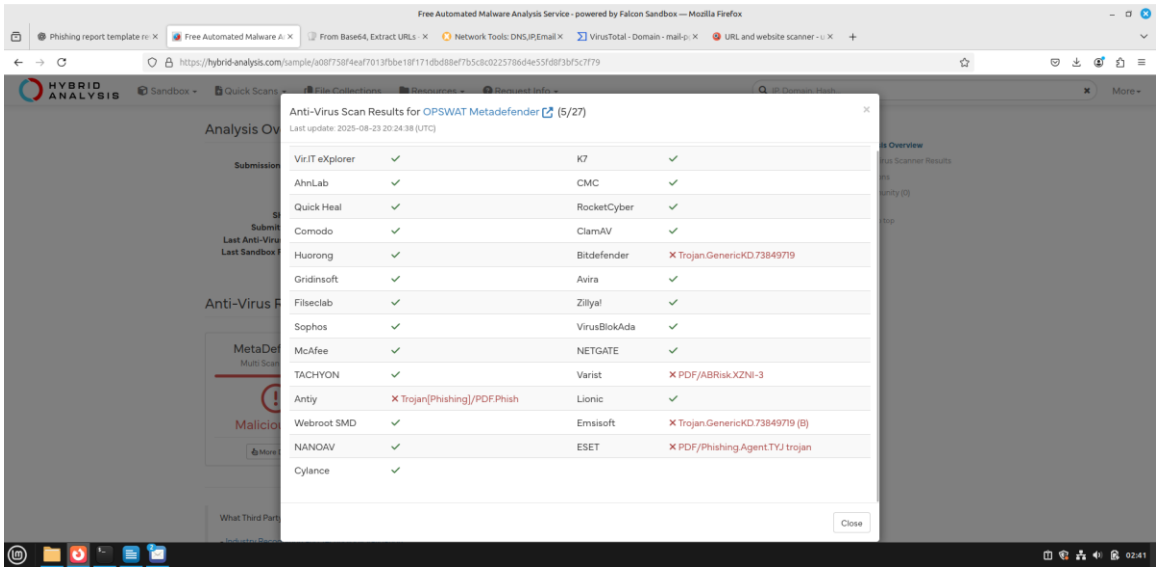
DMARC: pass action=none header.from=gmail.com

URL Analysis:

1) hxxps[://]plqwplwwllwl[.]z13[.]web[.]core[.]windows[.]net

The following URL is defanged in order to prevent accidental opening.





Attachment Analysis:

File Name: sample-1_4tAVSEUdcdaiO.pdf

Size: 129 KiB (131945 bytes)

Type: PDF

Description: PDF document, version 1.4, 1 page(s) (zip deflate encoded)

Document Creator: IronPdf

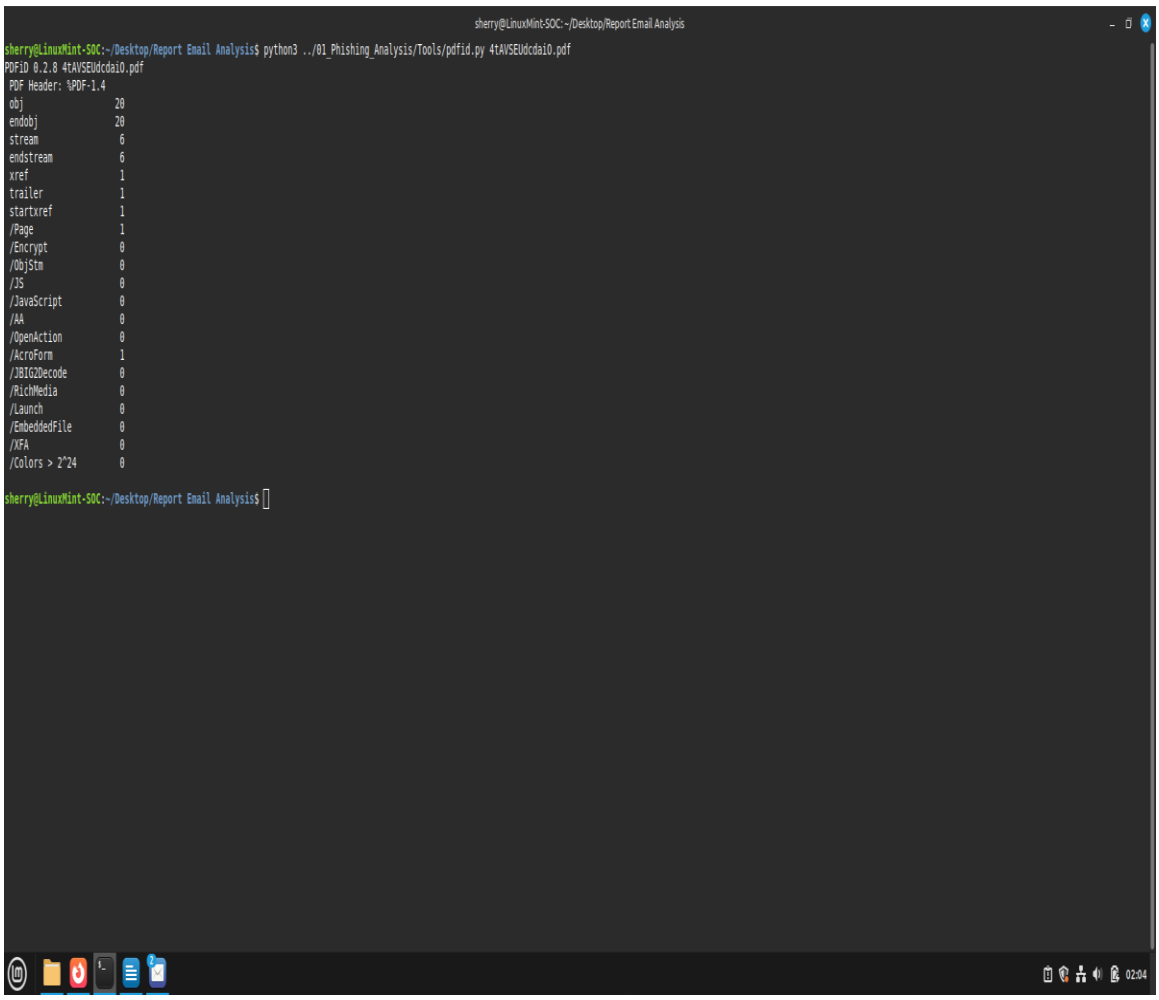
Document Producer: IronPdf v2022.11.10299

Document Pages: 1

MD5: d3a472a7f96cfb2a8536d4b0b14aa034

SHA1: 549a052fff4d920ed9ec6b67aee3832e54525922

SHA256:330445344ffbec313fbc0c87a8eac45c39b12b0d008c27be928ba06f2968f42a



BANCO DO BRASIL

BLOQUEIO EM CARTÃO E CONTA.

O Banco do Brasil identificou uma tentativa de movimentação suspeita e por segurança bloqueamos preventivamente sua conta e cartão.

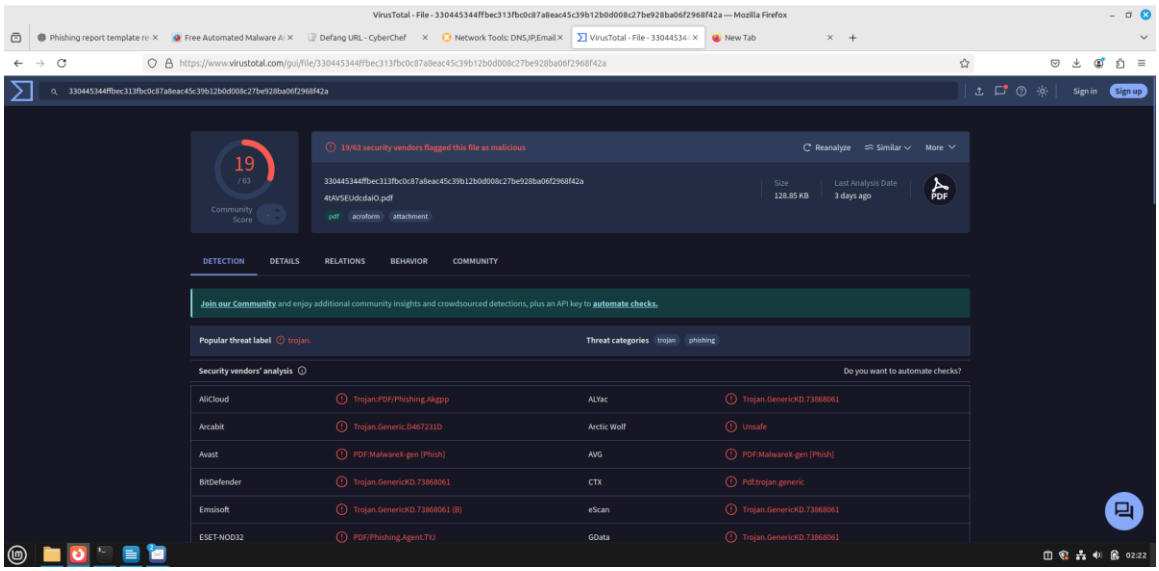
Efetue a liberação clicando abaixo.

Liberação

Efetue o procedimento de liberação para poder utilizar todas as funções de sua conta e cartão.

Banco do Brasil S.A CNPJ: 00.000.000/0001-91

t3f1IoNyZHDsZndS2uB



YARA Detection:

Signature: High Entropy File

Relevance: 5/10

ATT&CK: T1027.013

Extracted Files:

1) File Name: Annss.dat

Filepath: %APPDATA%\Adobe\Acrobat\11.0\Security\Annss.dat

Size: 10 KiB (10240 bytes)

Type: Unknown

Runtime Process: AcroRd32.exe (PID: 5188)

MD5: 5905c9b785a074e784ed0d133e728ca0

SHA1: d7b06c004a22446e8b6d8a49ebf0bfacc17d9e32

SHA256:d12d1bd6103cfdbb28e7d299342912a7111d97317bb1ad5ea758e0796b93dfeb

2) File Name: Annssi.dat

Filepath: %APPDATA%\Adobe\Acrobat\11.0\Security\Annssi.dat

Size: 24 KiB (24152 bytes)

Type: Unknown

Runtime Process: AcroRd32.exe (PID: 5188)

MD5: f51dcf54443d032e88650427dac8cdd3

SHA1: 7ae45594aac238c205e8524e670f50cb14e0eea4

SHA256:b8698f0727f20efbb69d733f52f07f2395b2f5f0c6fb2041d89bd0c56dd32bea

3) File Name: Annssk.dat

Filepath: %APPDATA%\Adobe\Acrobat\11.0\Security\Annssk.dat

Size: 264 B (264 bytes)

Type: Unknown

Runtime Process: AcroRd32.exe (PID: 5188)

MD5: 707aeaa64a0d19779f48d8dceebcf1ff

SHA1: f7f65b1cf734723d77c140f44f2c418c83e04f88

SHA256:8b88aca362dd9ed7889a7752f94337fda193c3e801619473d2bdeb1f59198bfb

Indicators of Compromise:

Sender IP reputation: Reported in Spam Campaign in August 2025.

Domain reputation: Reported in Spam Campaign in May 2024.

Email sample hash: c44bc0b8614423b8db74337ce795500de5fb71a4

URL: hxxps[://]plqwplwwllwl[.]z13[.]web[.]core[.]windows[.]net

Files: 1) Annss.dat

2) Annssi.dat

3) Annssk.dat

Potential Impact:

- Credential theft as the PDF contains a phishing Trojan that can steal user credentials.
- Malware infection as the PDF contains multiple .dat files and Trojans.

Verdict:

Result: Malicious (Phishing with Trojan payload)

Confidence: High

Defense Actions:

- Blocked sender IP/domain at the firewall and email server level to prevent additional phishing attempts.
- Quarantined the phishing email from the affected user's mailbox and deleted any similar messages found during a mailbox sweep.
- Alerted the targeted user (Cynthia), providing phishing awareness guidance to avoid interaction with suspicious emails in the future.
- Reported malicious indicators (IP, domain, file hashes) to abuse contacts and external threat intelligence sources.
- Monitored endpoints where the attachment may have been opened for signs of compromise, unusual processes, or persistence mechanisms.
- Updated security monitoring rules in the SIEM to flag similar phishing attempts.