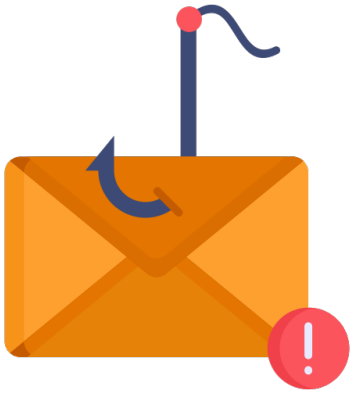
Phishing Email Analysis Report



Case: COMMERCIAL PURCHASE RECEIPT ONLINE 27 NOV

Date: October 2025

Prepared by: A. Brito

1. Introduction

During my time as part of the Security Operations Center (SOC) team at a higher education institution, I had the opportunity to work on real-world security incidents, many of which involved phishing attempts. In fact, phishing was one of the most frequent types of tickets I handled during my internship with the SOC team. While this scenario is fictional and designed for a cybersecurity lab, it closely reflects the kinds of phishing cases I encountered in an operational environment. This project serves to replicate that experience in a structured, documented format.

2. Executive Summary

A phishing email impersonating a purchase receipt notification was analyzed. The email originated from a spoofed university domain (uptc.edu.co) and failed SPF/DKIM authentication. It contained a link to a numeric IP hosting an executable payload. The email used common phishing tactics such as urgency, financial lures, and forged branding. The payload was determined to be malicious.

3. Incident Overview

Date of email: December 9, 2022

Subject: COMMERCIAL PURCHASE RECEIPT ONLINE 27 NOV

Sender: erikajohana.lopez@uptc.edu.co

Target: undisclosed-recipients

Threat Type: Phishing / Malware Delivery

Payload: http://107.175.247.199/loader/install.exe (.exe file)

```
From: ERIKA JOHANA LOPEZ VALIENTE <erikajohana.lopez@uptc.edu.co>
Date: |-
  Fri, 09 Dec 2022 09:58:26 +0100
Message-ID: <CABWu4iua5_uex6=G8pi_OJz1tBLJiNakMK-1=7128orpzxbKxw@mail.gmail.com>
Subject: COMMERCIAL PURCHASE RECEIPT ONLINE 27 NOV
To: |-
  undisclosed-recipients:;
```

4. Email Header Analysis

Authentication results:

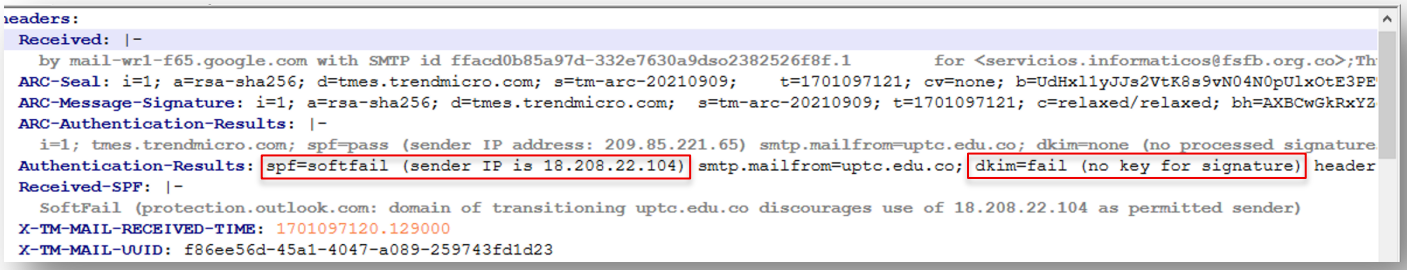
- **SPF:** softfail (sender IP 18.208.22.104)

- **DKIM:** fail (no valid key)

- **DMARC:** none

- **ARC:** fail

These results indicate the email is not authorized to be sent on behalf of the domain, a strong indicator of spoofing.



5. Email Body and Payload Analysis

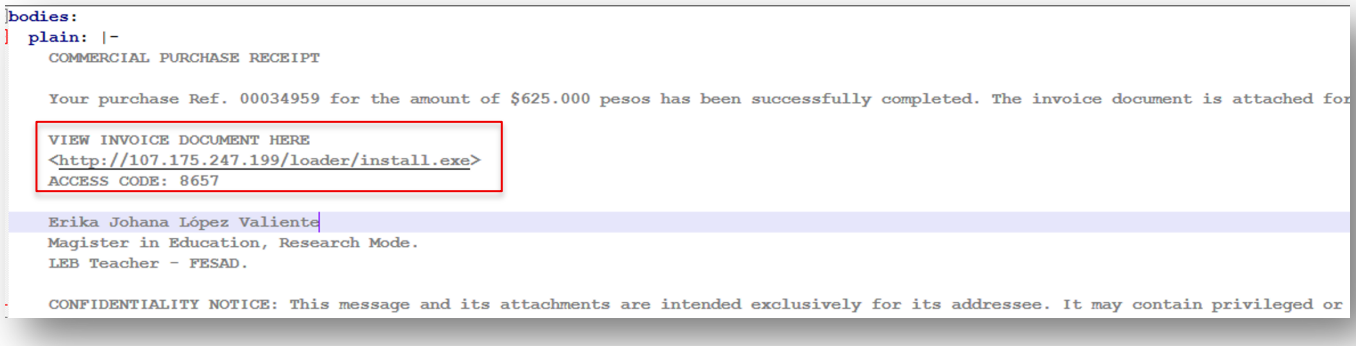
The body contained a message claiming a successful purchase of $625.000 pesos. The recipient was instructed to view an invoice via a malicious URL hosted at a numeric IP. The URL points to an executable file (.exe), which is a clear red flag.

Malicious URL: http://107.175.247.199/loader/install.exe

Access Code: 8657

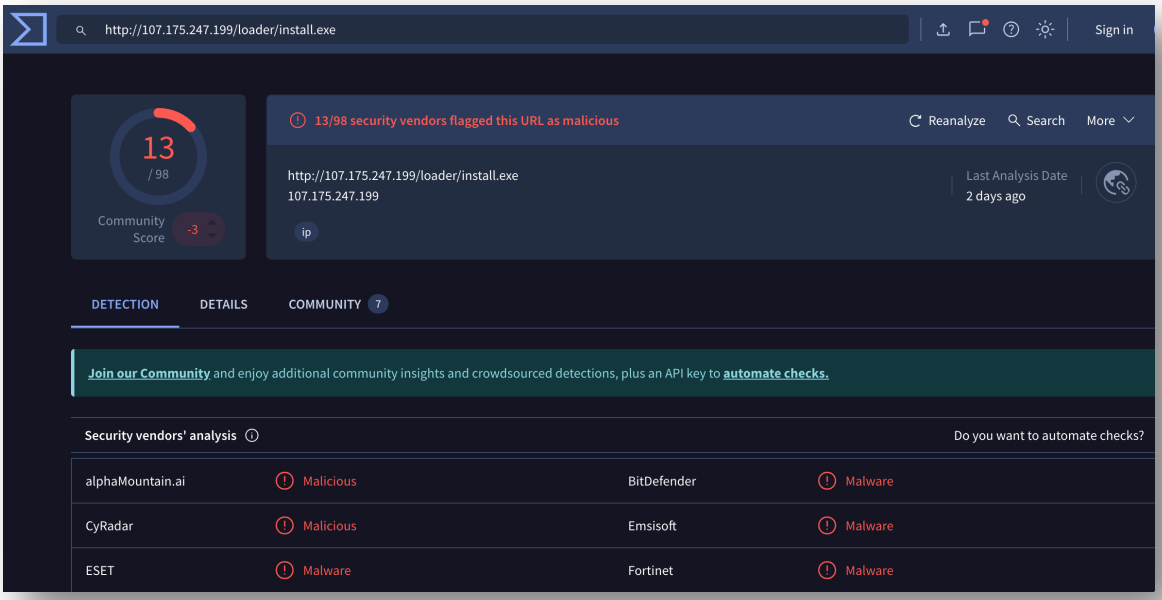
Branding: UPTC logo from Wikipedia used to appear legitimate.

The email included a confidentiality disclaimer to create a false sense of legitimacy.

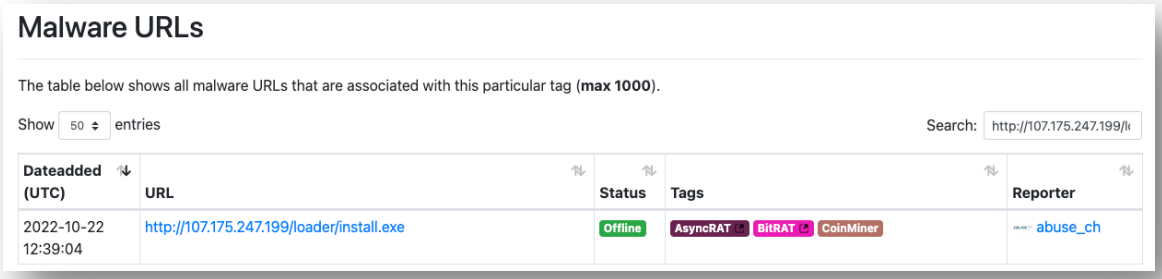


URL Analysis:

Virus Total



Abuse_Ch URL haus



6. Indicators of Compromise (IOCs)

IOC Type	Value
Sender Email	erikajohana.lopez@uptc.edu.co
Subject	COMMERCIAL PURCHASE RECEIPT ONLINE 27 NOV
Malicious URL	http://107.175.247.199/loader/install.exe
Access Code	8657
Source IP	18.208.22.104 (SPF softfail)
Message-ID	<CABWu4iua5_uex6=G8pi_OJz1tBLJiNakMK-1=7128orpzxbKxw@mail.gmail.com>

7. Detection Rules and Hunting Queries

Sample Microsoft Sentinel (KQL) query:

```
EmailEvents
| where Subject has "COMMERCIAL PURCHASE RECEIPT" or Subject has "PURCHASE RECEIPT"
| extend urls = extract_all(@"https?://[^\s'"<>]+", 0, Body)
| mv-expand urls
| where urls has "107.175.247.199" or urls has ".exe"
| project TimeGenerated, Subject, SenderFromAddress, RecipientEmailAddress, urls
| sort by TimeGenerated desc
```

8. Forensic & Sandbox Playbook

- Preserve original .eml and compute hashes.

- Extract URLs and attachments with tools such as ripmime or munpack.

- Submit the executable to a sandbox (e.g., Any.Run, Cuckoo) for dynamic analysis.

- Collect network indicators, process trees, and dropped files.

- Perform static analysis on the binary (strings, hash, PEID).

- Document findings and IOCs for SIEM ingestion.

9. Remediation & Lessons Learned

1. Block access to http://107.175.247.199 and related infrastructure.
2. Quarantine similar emails and add domain/IP to blocklists.
3. Implement email filters to flag emails with direct IP links or .exe attachments.
4. Notify users and conduct awareness training.
5. Monitor for post-exploitation activity if the payload was executed.

10. Appendix – Lab Source

This phishing scenario is based on the “PhishStrike Lab” from CyberDefenders.org, a hands-on cybersecurity training platform. The lab focuses on analyzing phishing emails to identify threat indicators, malware delivery mechanisms, and potential command-and-control (C2) channels. In this exercise, the scenario involves a phishing email targeting faculty members at an educational institution. The email impersonates a trusted contact and claims a $625,000 purchase, directing recipients to a malicious link to download a fake invoice. As the analyst, the objective is to investigate the email headers, inspect the payload, extract Indicators of Compromise (IOCs), and document findings—mirroring a real-world phishing investigation and response process.