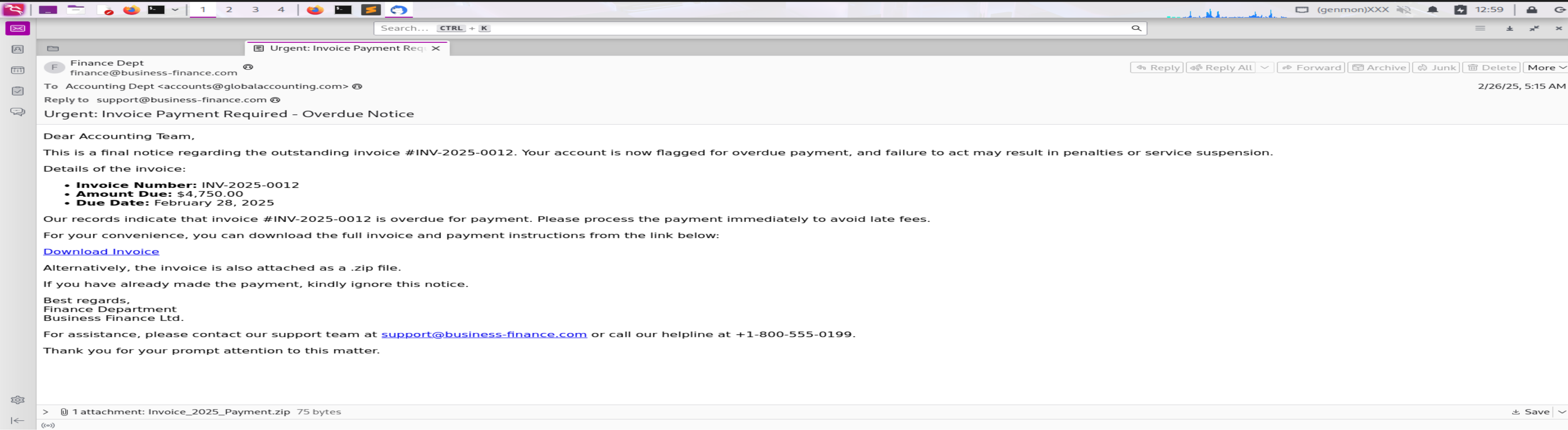


Finance Dept
finance@business-finance.com

To Accounting Dept <accounts@globalaccounting.com>

Reply to support@business-finance.com

2/26/25, 5:15 AM

Urgent: Invoice Payment Required - Overdue Notice

Dear Accounting Team,

This is a final notice regarding the outstanding invoice #INV-2025-0012. Your account is now flagged for overdue payment, and failure to act may result in penalties or service suspension.

Details of the invoice:

- **Invoice Number:** INV-2025-0012
- **Amount Due:** $4,750.00
- **Due Date:** February 28, 2025

Our records indicate that invoice #INV-2025-0012 is overdue for payment. Please process the payment immediately to avoid late fees.

For your convenience, you can download the full invoice and payment instructions from the link below:

Download Invoice

Alternatively, the invoice is also attached as a .zip file.

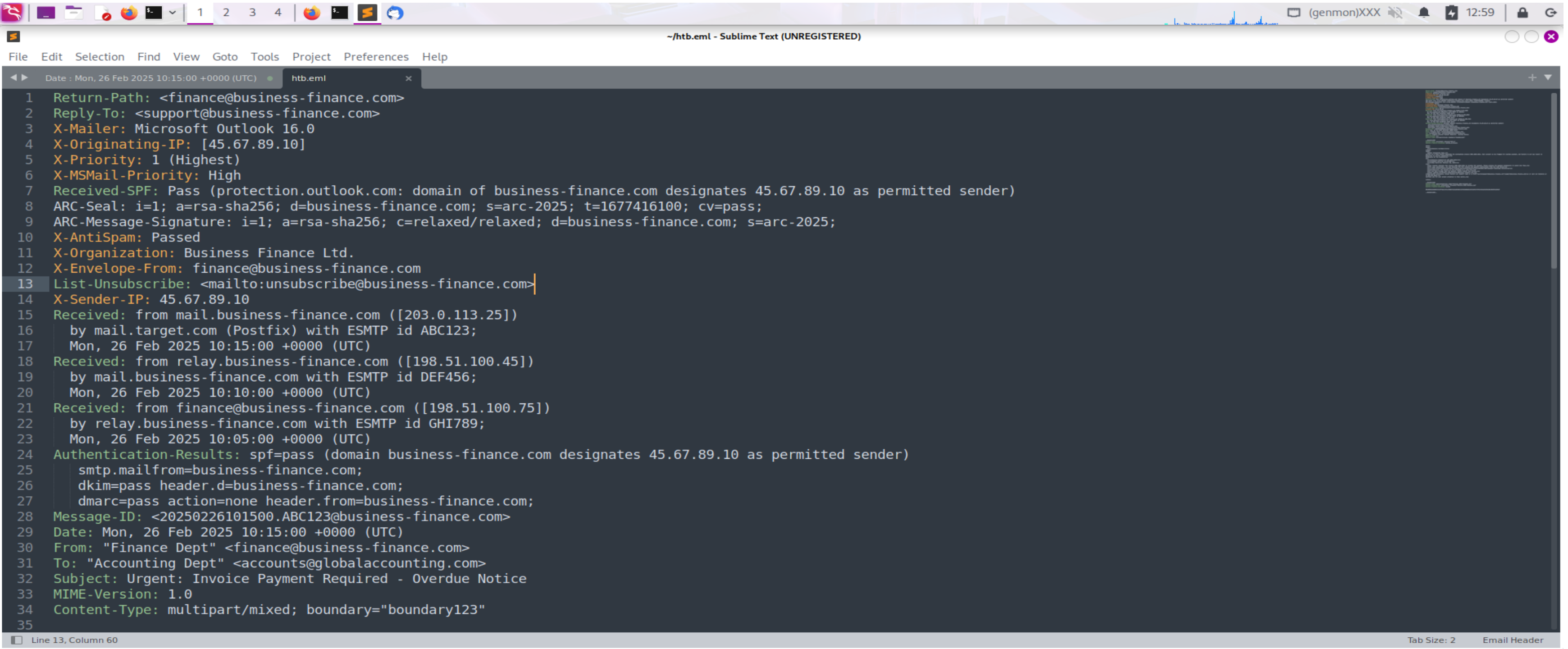
If you have already made the payment, kindly ignore this notice.

Best regards,
Finance Department
Business Finance Ltd.

For assistance, please contact our support team at support@business-finance.com or call our helpline at +1-800-555-0199.

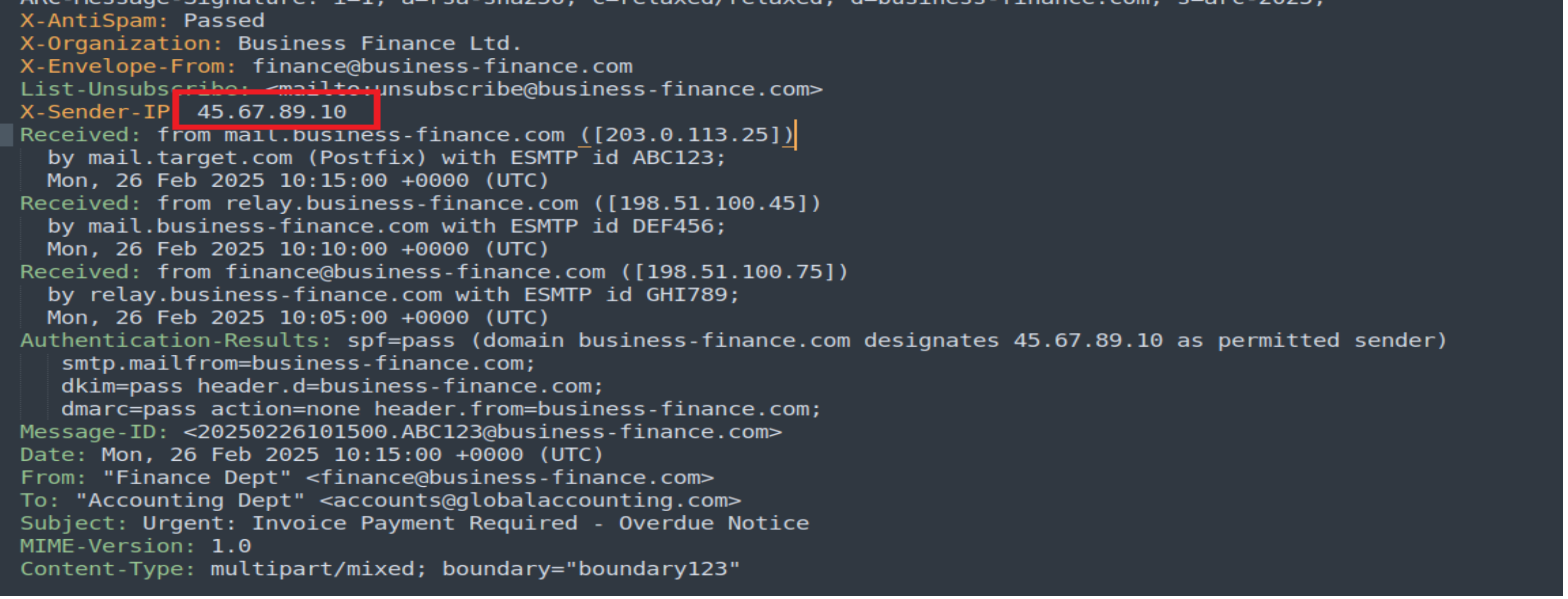
Thank you for your prompt attention to this matter.

> 1 attachment: Invoice_2025_Payment.zip 75 bytes


~/htb.eml - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
Date : Mon, 26 Feb 2025 10:15:00 +0000 (UTC)
htb.eml
Line 13, Column 60
Tab Size: 2
Email Header

```
Return-Path: <finance@business-finance.com>
Reply-To: <support@business-finance.com>
X-Mailer: Microsoft Outlook 16.0
X-Originating-IP: [45.67.89.10]
X-Priority: 1 (Highest)
X-MSMail-Priority: High
Received-SPF: Pass (protection.outlook.com: domain of business-finance.com designates 45.67.89.10 as permitted sender)
ARC-Seal: i=1; a=rsa-sha256; d=business-finance.com; s=arc-2025; t=1677416100; cv=pass;
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=business-finance.com; s=arc-2025;
X-AntiSpam: Passed
X-Organization: Business Finance Ltd.
X-Envelope-From: finance@business-finance.com
List-Unsubscribe: <mailto:unsubscribe@business-finance.com>
X-Sender-IP: 45.67.89.10
Received: from mail.business-finance.com ([203.0.113.25])
  by mail.target.com (Postfix) with ESMTP id ABC123;
  Mon, 26 Feb 2025 10:15:00 +0000 (UTC)
Received: from relay.business-finance.com ([198.51.100.45])
  by mail.business-finance.com with ESMTP id DEF456;
  Mon, 26 Feb 2025 10:10:00 +0000 (UTC)
Received: from finance@business-finance.com ([198.51.100.75])
  by relay.business-finance.com with ESMTP id GHI789;
  Mon, 26 Feb 2025 10:05:00 +0000 (UTC)
Authentication-Results: spf=pass (domain business-finance.com designates 45.67.89.10 as permitted sender)
   smtp.mailfrom=business-finance.com;
   dkim=pass header.d=business-finance.com;
   dmarc=pass action=none header.from=business-finance.com;
Message-ID: <20250226101500.ABC123@business-finance.com>
Date: Mon, 26 Feb 2025 10:15:00 +0000 (UTC)
From: "Finance Dept" <finance@business-finance.com>
To: "Accounting Dept" <accounts@globalaccounting.com>
Subject: Urgent: Invoice Payment Required - Overdue Notice
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="boundary123"
```

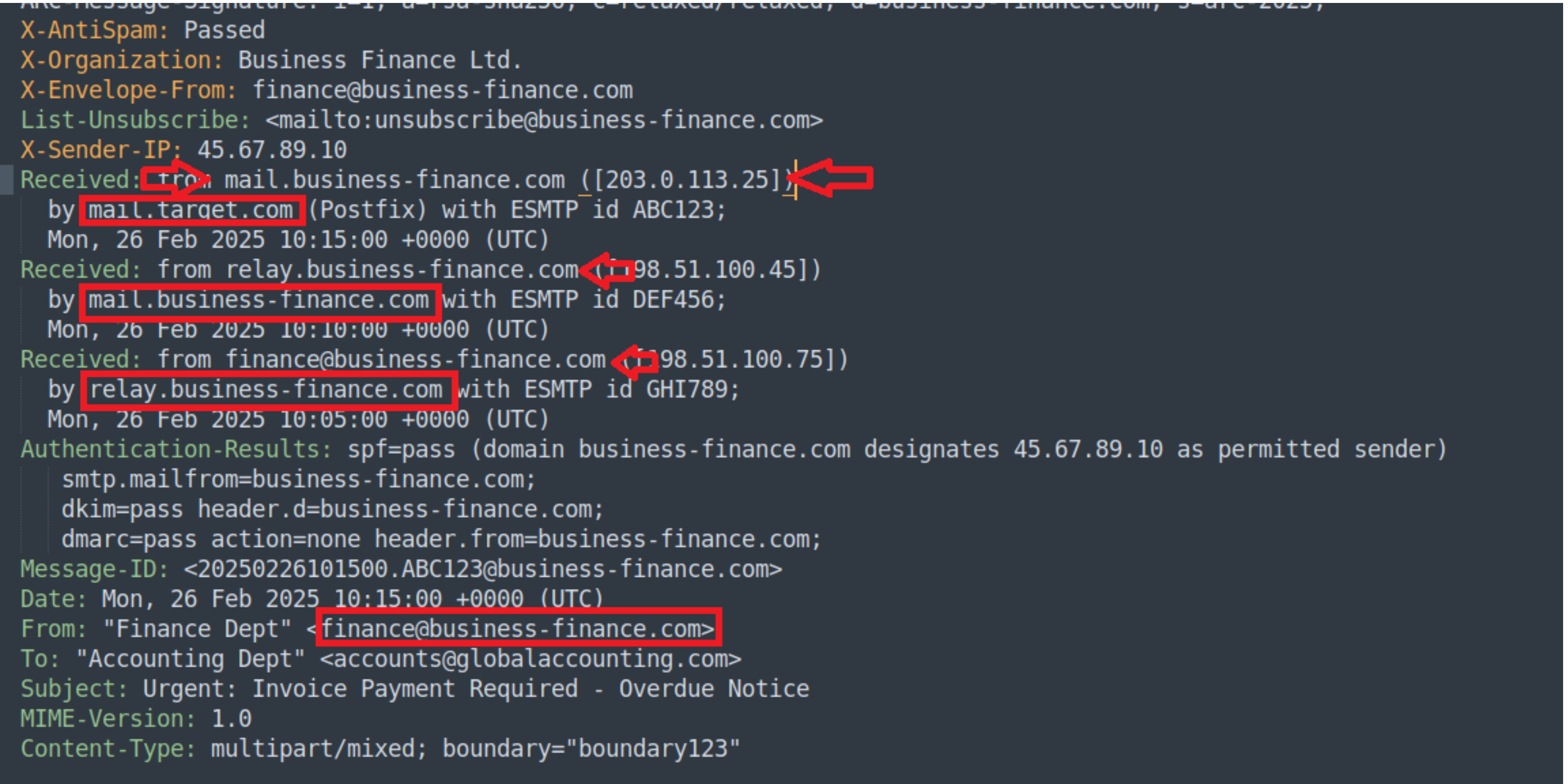
Opened the email in both Thunderbird
And sublime text



```
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=business-finance.com; s=arc-2025;
X-AntiSpam: Passed
X-Organization: Business Finance Ltd.
X-Envelope-From: finance@business-finance.com
List-Unsubscribe: <mailto:unsubscribe@business-finance.com>
X-Sender-IP: 45.67.89.10
Received: from mail.business-finance.com ([203.0.113.25])
  by mail.target.com (Postfix) with ESMTP id ABC123;
  Mon, 26 Feb 2025 10:15:00 +0000 (UTC)
Received: from relay.business-finance.com ([198.51.100.45])
  by mail.business-finance.com with ESMTP id DEF456;
  Mon, 26 Feb 2025 10:10:00 +0000 (UTC)
Received: from finance@business-finance.com ([198.51.100.75])
  by relay.business-finance.com with ESMTP id GHI789;
  Mon, 26 Feb 2025 10:05:00 +0000 (UTC)
Authentication-Results: spf=pass (domain business-finance.com designates 45.67.89.10 as permitted sender)
   smtp.mailfrom=business-finance.com;
   dkim=pass header.d=business-finance.com;
   dmarc=pass action=none header.from=business-finance.com;
Message-ID: <20250226101500.ABC123@business-finance.com>
Date: Mon, 26 Feb 2025 10:15:00 +0000 (UTC)
From: "Finance Dept" <finance@business-finance.com>
To: "Accounting Dept" <accounts@globalaccounting.com>
Subject: Urgent: Invoice Payment Required - Overdue Notice
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="boundary123"
```

What is the sender IP – 45.67.89.10

What is the sender's email address – finance@business-finance.com



```
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=business-finance.com; s=arc-2025;
X-AntiSpam: Passed
X-Organization: Business Finance Ltd.
X-Envelope-From: finance@business-finance.com
List-Unsubscribe: <mailto:unsubscribe@business-finance.com>
X-Sender-IP: 45.67.89.10
Received: from mail.business-finance.com ([203.0.113.25])
  by mail.target.com (Postfix) with ESMTP id ABC123;
  Mon, 26 Feb 2025 10:15:00 +0000 (UTC)
Received: from relay.business-finance.com ([198.51.100.45])
  by mail.business-finance.com with ESMTP id DEF456;
  Mon, 26 Feb 2025 10:10:00 +0000 (UTC)
Received: from finance@business-finance.com ([198.51.100.75])
  by relay.business-finance.com with ESMTP id GHI789;
  Mon, 26 Feb 2025 10:05:00 +0000 (UTC)
Authentication-Results: spf=pass (domain business-finance.com designates 45.67.89.10 as permitted sender)
   smtp.mailfrom=business-finance.com;
   dkim=pass header.d=business-finance.com;
   dmarc=pass action=none header.from=business-finance.com;
Message-ID: <20250226101500.ABC123@business-finance.com>
Date: Mon, 26 Feb 2025 10:15:00 +0000 (UTC)
From: "Finance Dept" <finance@business-finance.com>
To: "Accounting Dept" <accounts@globalaccounting.com>
Subject: Urgent: Invoice Payment Required - Overdue Notice
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="boundary123"
```

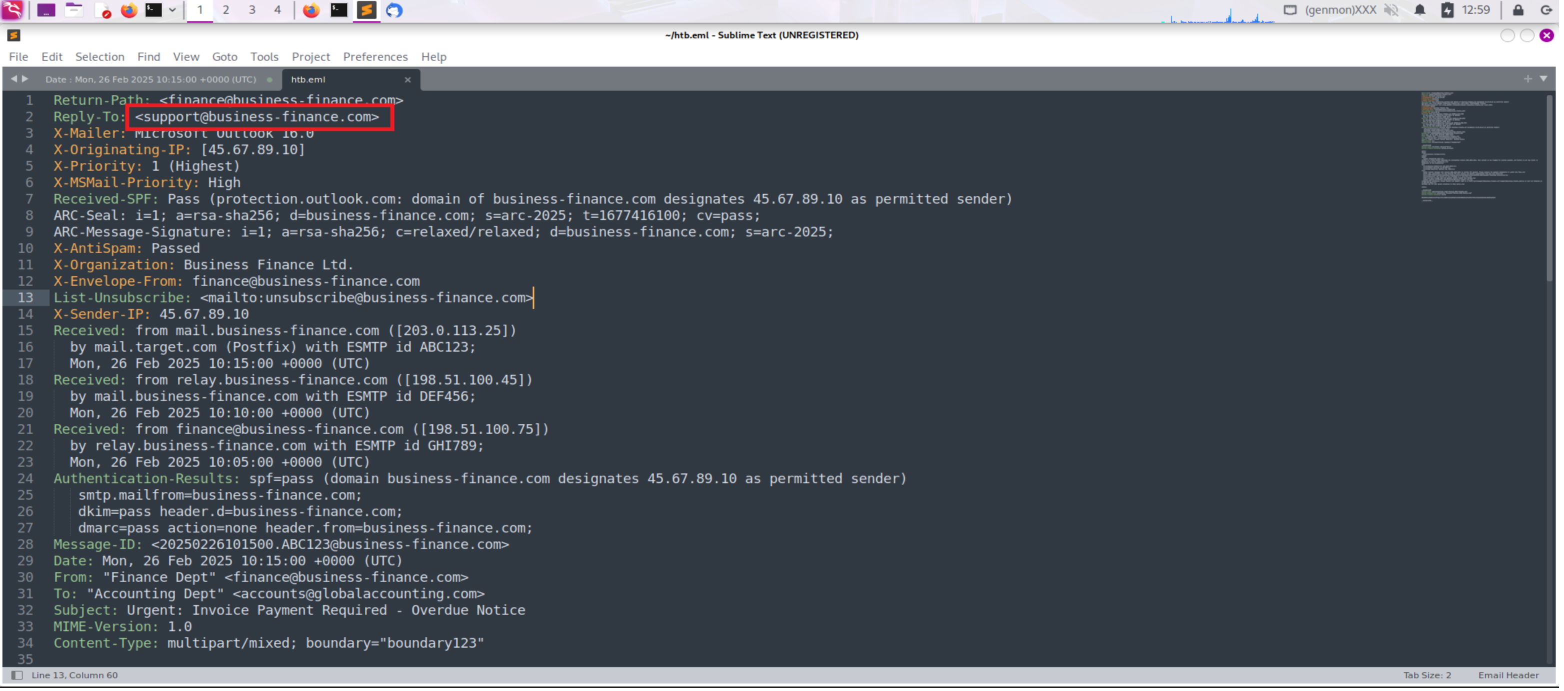
Which mail server relayed this email before reaching the victim?

So basically, it's from bottom to top

The from address is from relay.business-finance.com

And that address is from the mail.business-finance.com

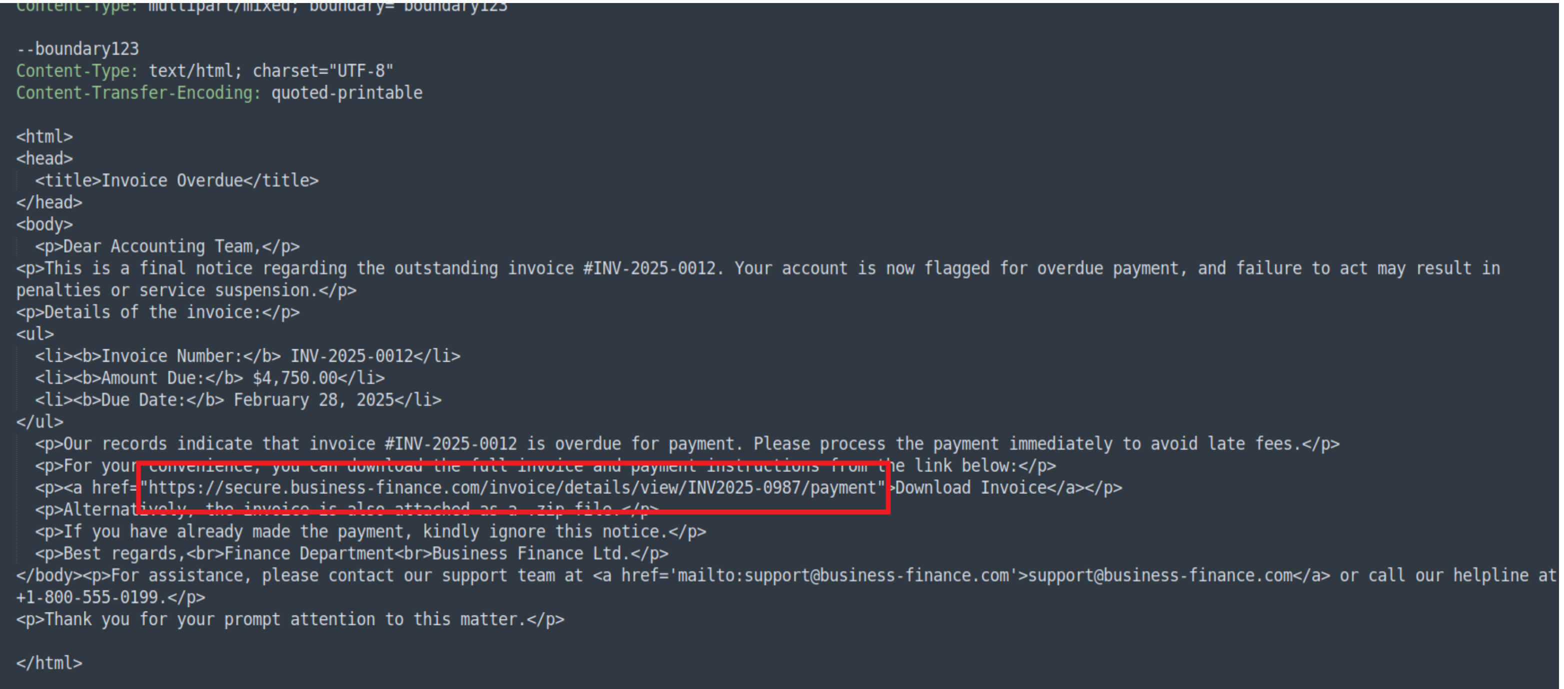
And that address is from mail.target.com (203.0.113.25)



```
Return-Path: <finance@business-finance.com>
Reply-To: <support@business-finance.com>
X-Mailer: Microsoft Outlook 16.0
X-Originating-IP: [45.67.89.10]
X-Priority: 1 (Highest)
X-MSMail-Priority: High
Received-SPF: Pass (protection.outlook.com: domain of business-finance.com designates 45.67.89.10 as permitted sender)
ARC-Seal: i=1; a=rsa-sha256; d=business-finance.com; s=arc-2025; t=1677416100; cv=pass;
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=business-finance.com; s=arc-2025;
X-AntiSpam: Passed
X-Organization: Business Finance Ltd.
X-Envelope-From: finance@business-finance.com
List-Unsubscribe: <mailto:unsubscribe@business-finance.com>
X-Sender-IP: 45.67.89.10
Received: from mail.business-finance.com ([203.0.113.25])
  by mail.target.com (Postfix) with ESMTP id ABC123;
  Mon, 26 Feb 2025 10:15:00 +0000 (UTC)
Received: from relay.business-finance.com ([198.51.100.45])
  by mail.business-finance.com with ESMTP id DEF456;
  Mon, 26 Feb 2025 10:10:00 +0000 (UTC)
Received: from finance@business-finance.com ([198.51.100.75])
  by relay.business-finance.com with ESMTP id GHI789;
  Mon, 26 Feb 2025 10:05:00 +0000 (UTC)
Authentication-Results: spf=pass (domain business-finance.com designates 45.67.89.10 as permitted sender)
   smtp.mailfrom=business-finance.com;
   dkim=pass header.d=business-finance.com;
   dmarc=pass action=none header.from=business-finance.com;
Message-ID: <20250226101500.ABC123@business-finance.com>
Date: Mon, 26 Feb 2025 10:15:00 +0000 (UTC)
From: "Finance Dept" <finance@business-finance.com>
To: "Accounting Dept" <accounts@globalaccounting.com>
Subject: Urgent: Invoice Payment Required - Overdue Notice
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="boundary123"
```

What is the reply-to email address?
support@business-finance.com

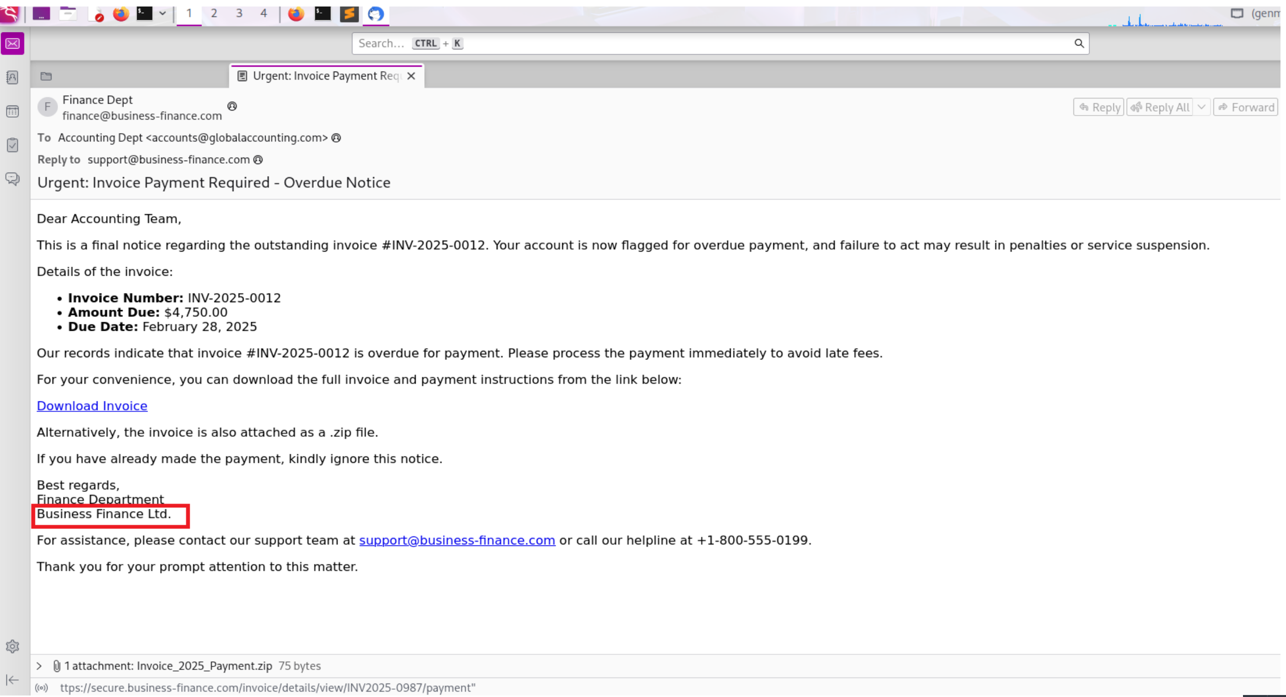
What is the SPF result for this email?
PASS



```
Content-Type: multipart/mixed; boundary="boundary123"

--boundary123
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable

<html>
<head>
  <title>Invoice Overdue</title>
</head>
<body>
  <p>Dear Accounting Team,</p>
<p>This is a final notice regarding the outstanding invoice #INV-2025-0012. Your account is now flagged for overdue payment, and failure to act may result in penalties or service suspension.</p>
<p>Details of the invoice:</p>
<ul>
  <li><b>Invoice Number:</b> INV-2025-0012</li>
  <li><b>Amount Due:</b> $4,750.00</li>
  <li><b>Due Date:</b> February 28, 2025</li>
</ul>
  <p>Our records indicate that invoice #INV-2025-0012 is overdue for payment. Please process the payment immediately to avoid late fees.</p>
  <p>For your convenience, you can download the full invoice and payment instructions from the link below:</p>
  <p><a href="https://secure.business-finance.com/invoice/details/view/INV2025-0987/payment">Download Invoice</a></p>
  <p>Alternatively, the invoice is also attached as a .zip file.</p>
  <p>If you have already made the payment, kindly ignore this notice.</p>
  <p>Best regards,<br>Finance Department<br>Business Finance Ltd.</p>
</body><p>For assistance, please contact our support team at <a href='mailto:support@business-finance.com'>support@business-finance.com</a> or call our helpline at +1-800-555-0199.</p>
<p>Thank you for your prompt attention to this matter.</p>

</html>
```

What is the domain used in the phishing
URL in the email

Secure.business-finance.com



Finance Dept
finance@business-finance.com

To Accounting Dept <accounts@globalaccounting.com>

Reply to support@business-finance.com

Urgent: Invoice Payment Required - Overdue Notice

Dear Accounting Team,

This is a final notice regarding the outstanding invoice #INV-2025-0012. Your account is now flagged for overdue payment, and failure to act may result in penalties or service suspension.

Details of the invoice:

- **Invoice Number:** INV-2025-0012
- **Amount Due:** $4,750.00
- **Due Date:** February 28, 2025

Our records indicate that invoice #INV-2025-0012 is overdue for payment. Please process the payment immediately to avoid late fees.

For your convenience, you can download the full invoice and payment instructions from the link below:

Download Invoice

Alternatively, the invoice is also attached as a .zip file.

If you have already made the payment, kindly ignore this notice.

Best regards,
Finance Department
Business Finance Ltd.

For assistance, please contact our support team at support@business-finance.com or call our helpline at +1-800-555-0199.

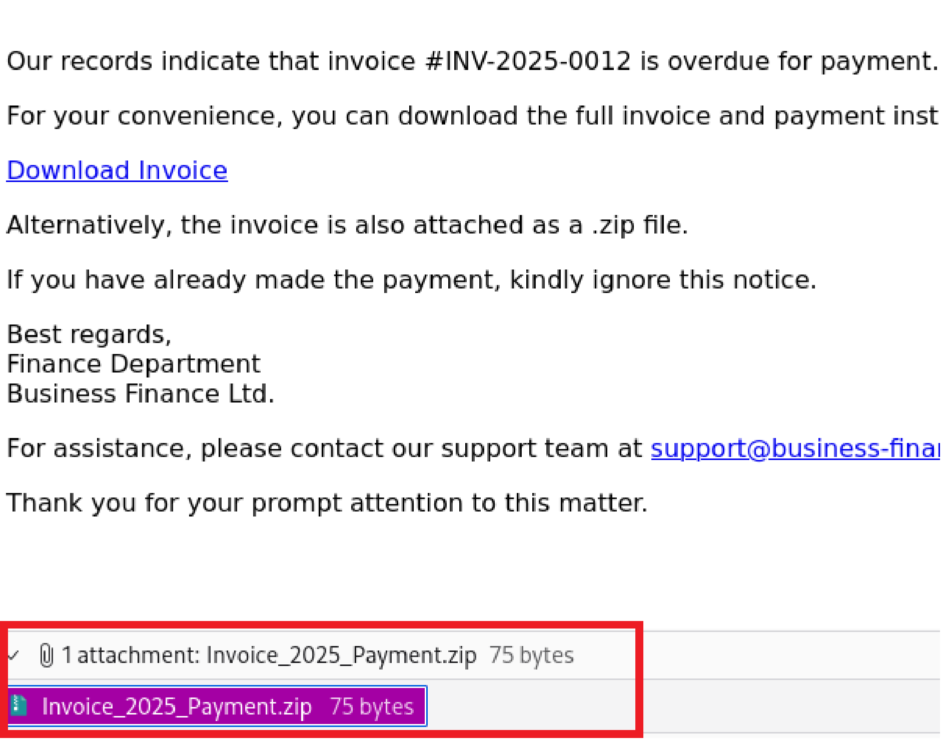
Thank you for your prompt attention to this matter.

1 attachment: Invoice_2025_Payment.zip 75 bytes

ttps://secure.business-finance.com/invoice/details/view/INV2025-0987/payment"

What is the fake company name used in the email?
- Business Finance Ltd.

What is the name of the attachment included in the email?
Invoice_2025_Payment.zip.



Our records indicate that invoice #INV-2025-0012 is overdue for payment.

For your convenience, you can download the full invoice and payment inst

Download Invoice

Alternatively, the invoice is also attached as a .zip file.

If you have already made the payment, kindly ignore this notice.

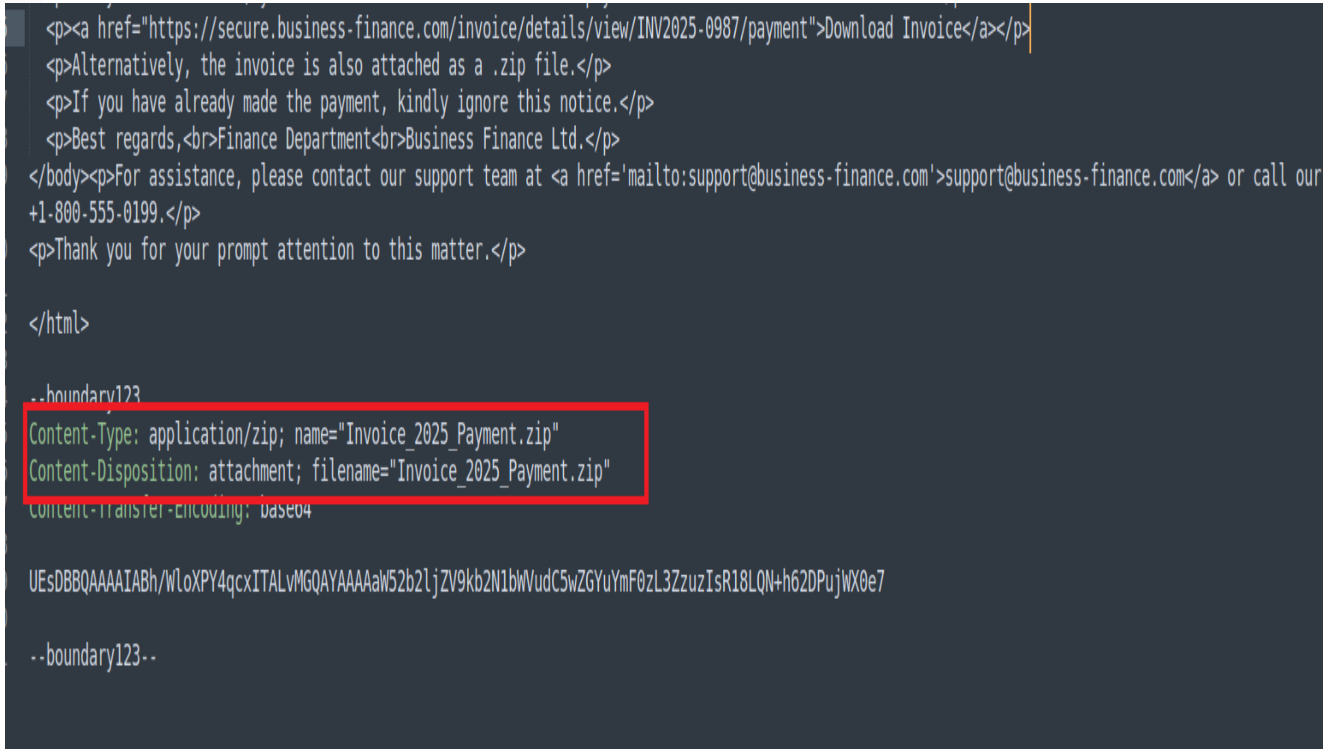
Best regards,
Finance Department
Business Finance Ltd.

For assistance, please contact our support team at support@business-fina

Thank you for your prompt attention to this matter.

1 attachment: Invoice_2025_Payment.zip 75 bytes

Invoice_2025_Payment.zip 75 bytes

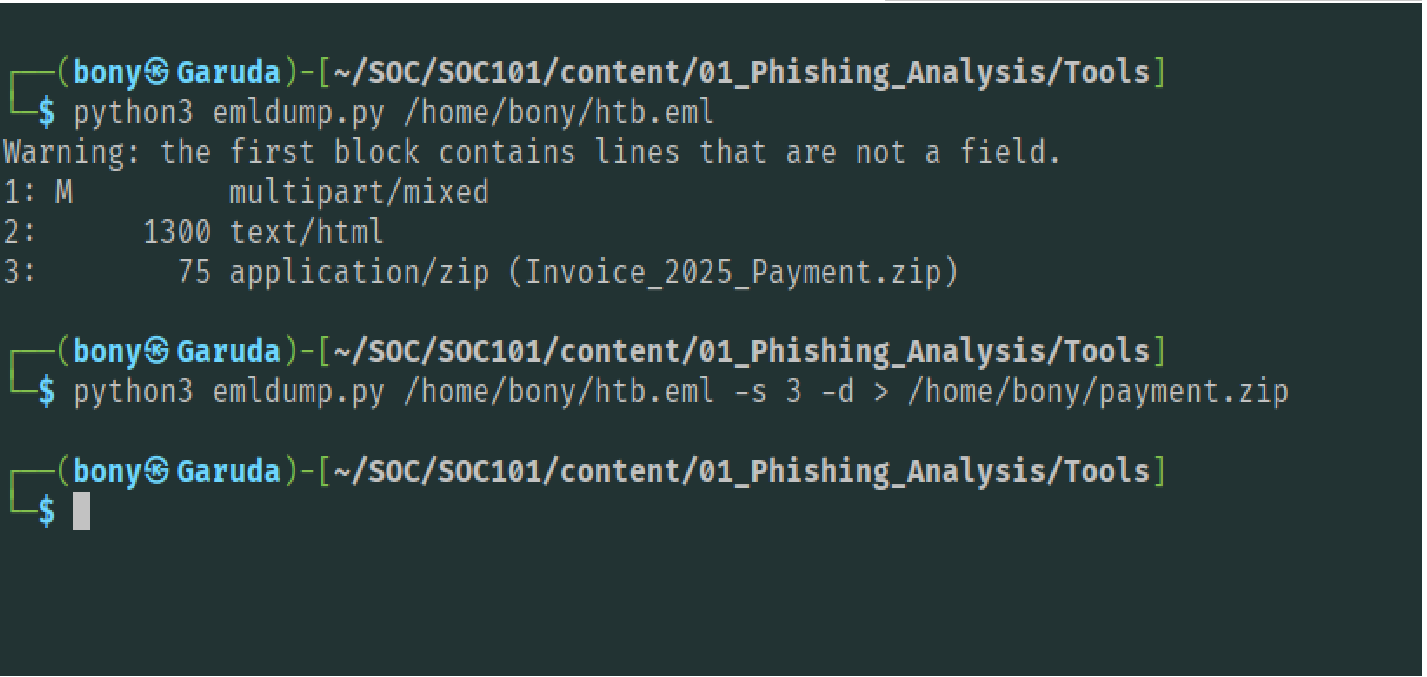


```
  <p><a href="https://secure.business-finance.com/invoice/details/view/INV2025-0987/payment">Download Invoice</a></p>
  <p>Alternatively, the invoice is also attached as a .zip file.</p>
  <p>If you have already made the payment, kindly ignore this notice.</p>
  <p>Best regards,<br>Finance Department<br>Business Finance Ltd.</p>
</body><p>For assistance, please contact our support team at <a href='mailto:support@business-finance.com'>support@business-finance.com</a> or call our
+1-800-555-0199.</p>
<p>Thank you for your prompt attention to this matter.</p>

</html>

--boundary123
Content-Type: application/zip; name="Invoice_2025_Payment.zip"
Content-Disposition: attachment; filename="Invoice_2025_Payment.zip"
Content-Transfer-Encoding: base64

UEsDBBQAAAAIABh/WloXPY4qcxITALvMGQAYAAAAaW52b2ljZV9kb2N1bWVudC5wZGYuYmF0zL3ZzuzIsR18LQN+h62DPujWX0e7

--boundary123--
```

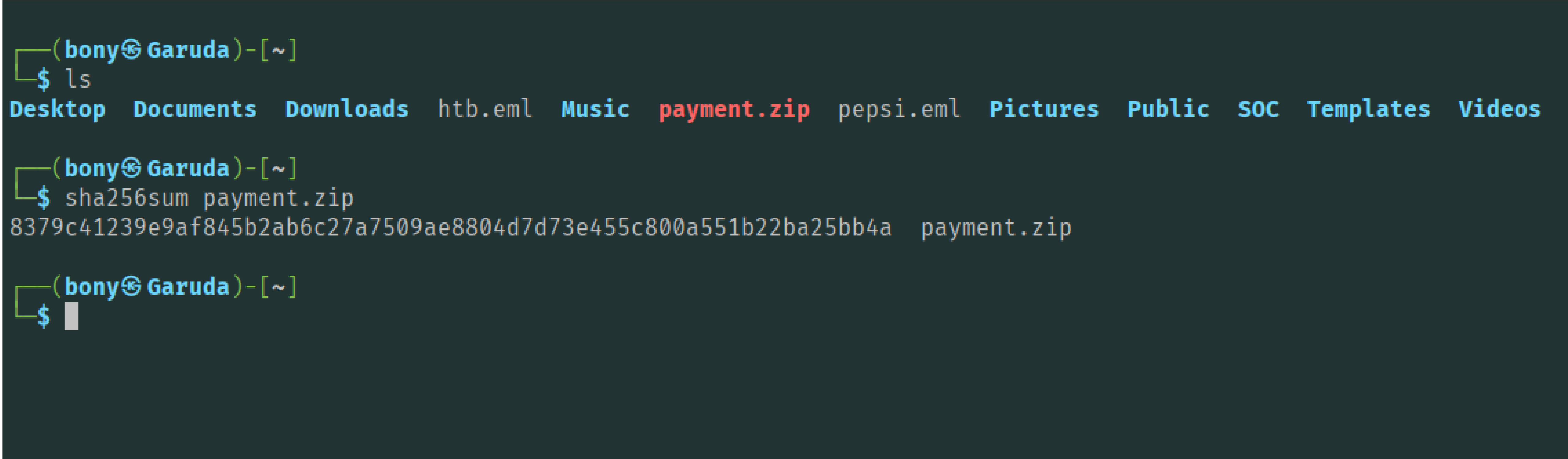
What is the SHA-256 hash of the attachment?

First, I used the emldump command to parse the Email files, then I selected the index where a zip file is present. Then I used –d to decompress it.

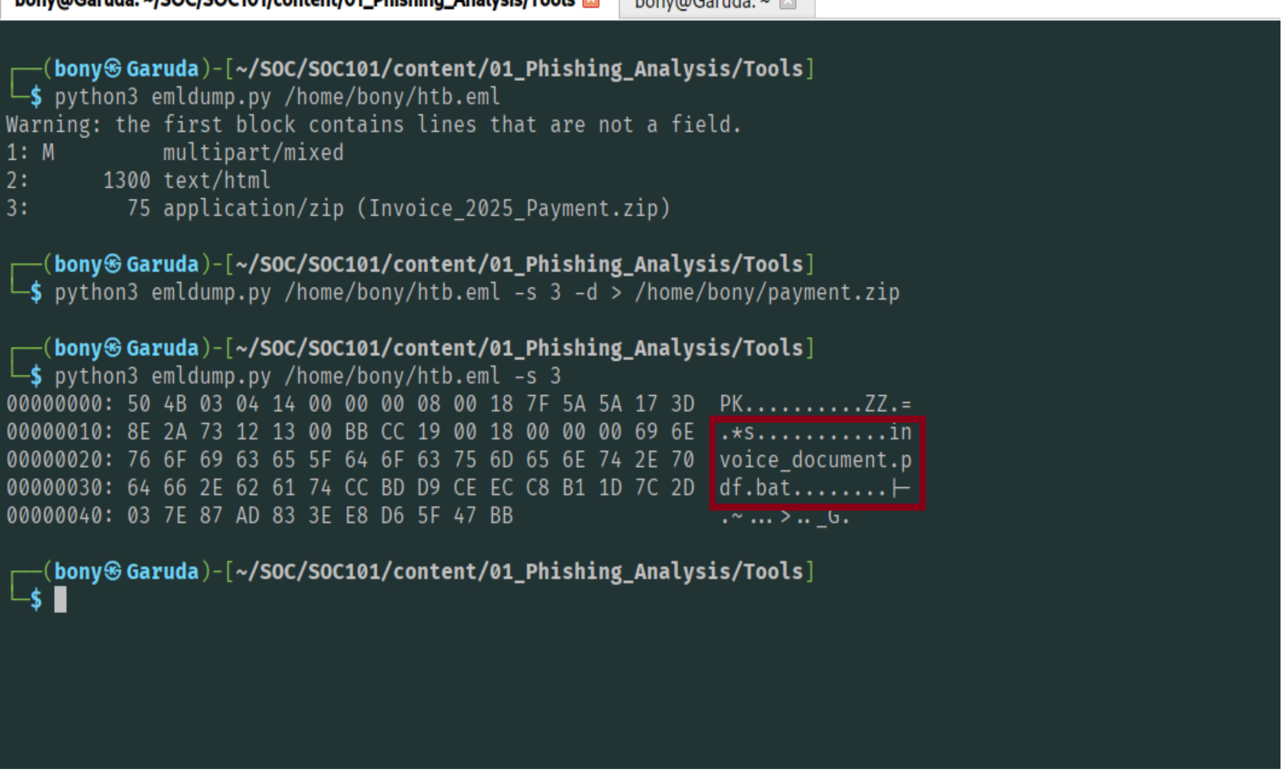
Then I used that decompressed file to get the hash By using sha256sum decompressed file name.



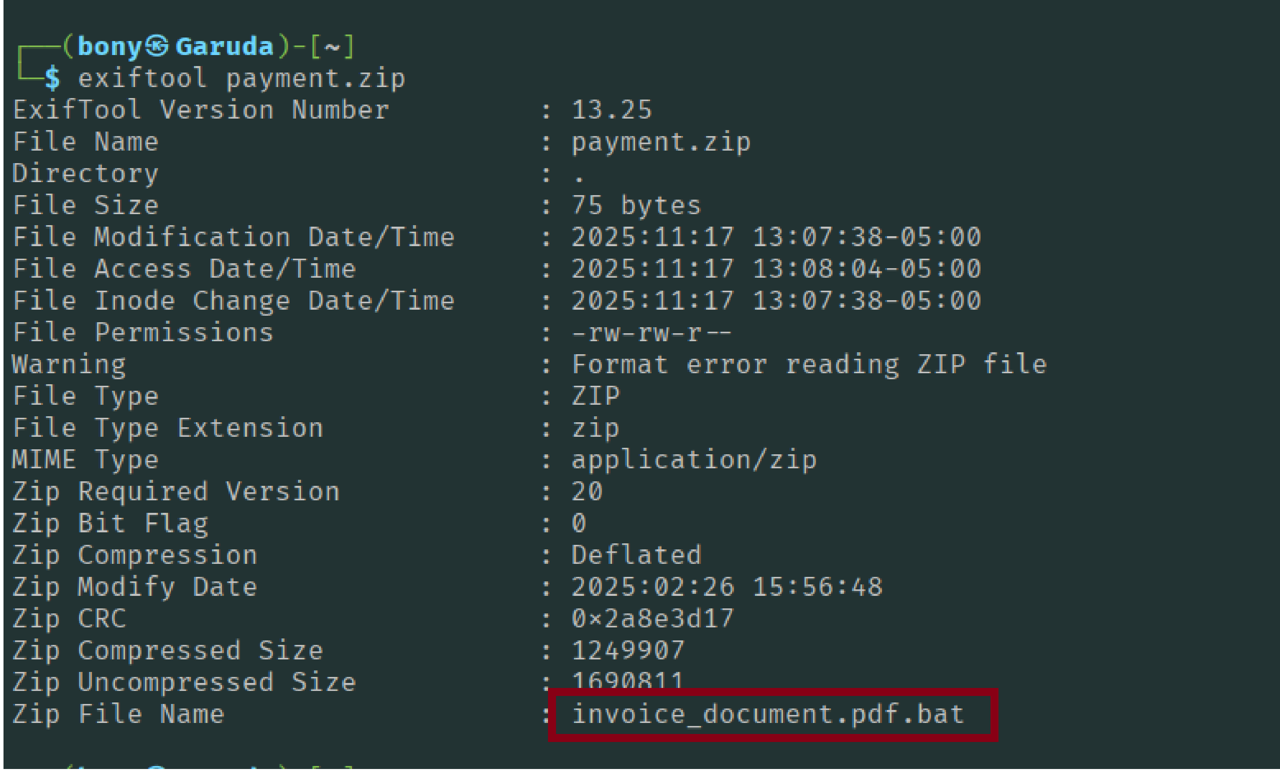
```
┌──(bony㉿Garuda)-[~/SOC/SOC101/content/01_Phishing_Analysis/Tools]
└─$ python3 emldump.py /home/bony/htb.eml
Warning: the first block contains lines that are not a field.
1: M         multipart/mixed
2:      1300 text/html
3:        75 application/zip (Invoice_2025_Payment.zip)

┌──(bony㉿Garuda)-[~/SOC/SOC101/content/01_Phishing_Analysis/Tools]
└─$ python3 emldump.py /home/bony/htb.eml -s 3 -d > /home/bony/payment.zip

┌──(bony㉿Garuda)-[~/SOC/SOC101/content/01_Phishing_Analysis/Tools]
└─$ 
```



```
┌──(bony㉿Garuda)-[~]
└─$ ls
Desktop  Documents  Downloads  htb.eml  Music  payment.zip  pepsi.eml  Pictures  Public  SOC  Templates  Videos

┌──(bony㉿Garuda)-[~]
└─$ sha256sum payment.zip
8379c41239e9af845b2ab6c27a7509ae8804d7d73e455c800a551b22ba25bb4a  payment.zip

┌──(bony㉿Garuda)-[~]
└─$ 
```

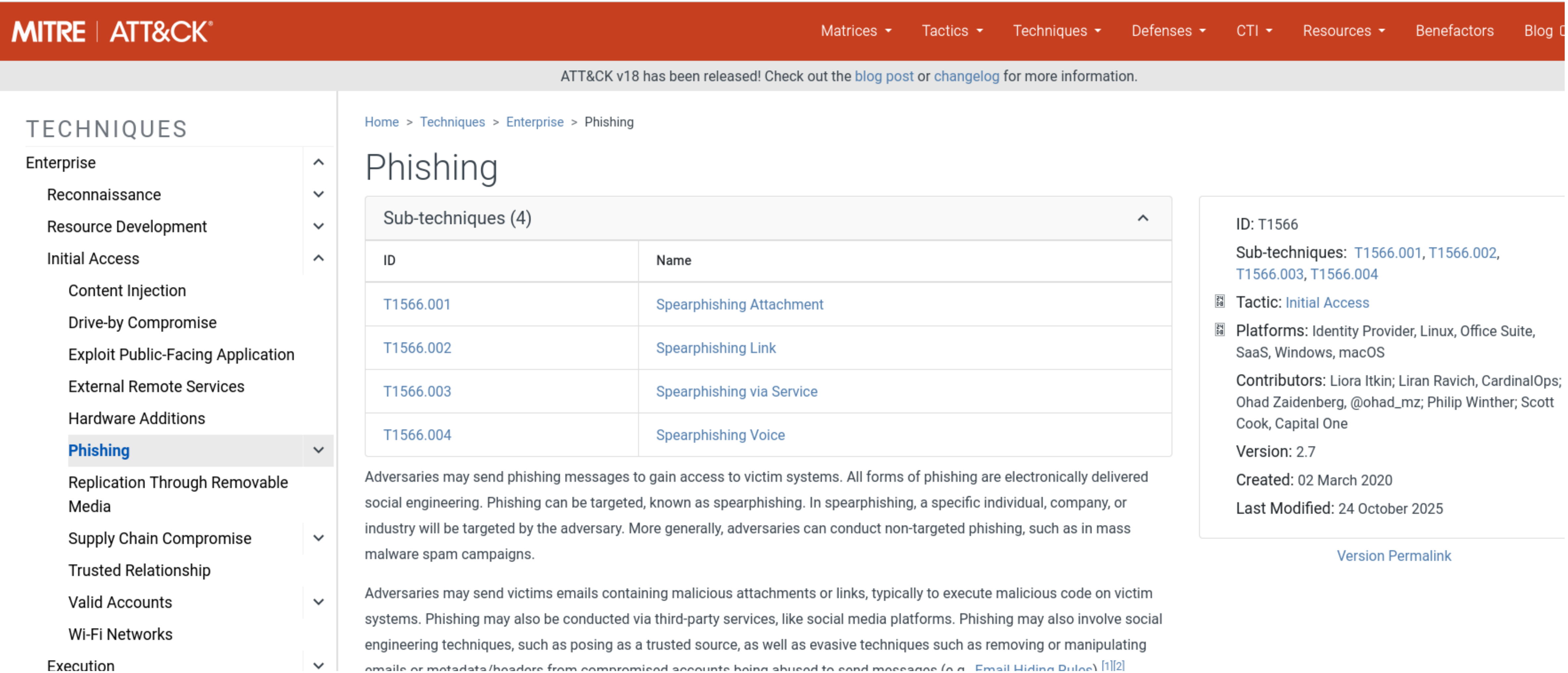

bony@Garuda: ~/SOC/SOC101/content/01_Phishing_Analysis/Tools
bony@Garuda: ~

```
┌──(bony㉿Garuda)-[~/SOC/SOC101/content/01_Phishing_Analysis/Tools]
└─$ python3 emldump.py /home/bony/htb.eml
Warning: the first block contains lines that are not a field.
1: M         multipart/mixed
2:      1300 text/html
3:        75 application/zip (Invoice_2025_Payment.zip)

┌──(bony㉿Garuda)-[~/SOC/SOC101/content/01_Phishing_Analysis/Tools]
└─$ python3 emldump.py /home/bony/htb.eml -s 3 -d > /home/bony/payment.zip

┌──(bony㉿Garuda)-[~/SOC/SOC101/content/01_Phishing_Analysis/Tools]
└─$ python3 emldump.py /home/bony/htb.eml -s 3
00000000: 50 4B 03 04 14 00 00 00 08 00 18 7F 5A 5A 17 3D  PK..........ZZ.=
00000010: 8E 2A 73 12 13 00 BB CC 19 00 18 00 00 00 69 6E  .*s...........in
00000020: 76 6F 69 63 65 5F 64 6F 63 75 6D 65 6E 74 2E 70  voice_document.p
00000030: 64 66 2E 62 61 74 CC BD D9 CE EC C8 B1 1D 7C 2D  df.bat........├
00000040: 03 7E 87 AD 83 3E E8 D6 5F 47 BB                 .~...>.._G.

┌──(bony㉿Garuda)-[~/SOC/SOC101/content/01_Phishing_Analysis/Tools]
└─$ 
```



```
┌──(bony㉿Garuda)-[~]
└─$ exiftool payment.zip
ExifTool Version Number         : 13.25
File Name                       : payment.zip
Directory                       : .
File Size                       : 75 bytes
File Modification Date/Time     : 2025:11:17 13:07:38-05:00
File Access Date/Time           : 2025:11:17 13:08:04-05:00
File Inode Change Date/Time     : 2025:11:17 13:07:38-05:00
File Permissions                : -rw-rw-r--
Warning                         : Format error reading ZIP file
File Type                       : ZIP
File Type Extension             : zip
MIME Type                       : application/zip
Zip Required Version            : 20
Zip Bit Flag                    : 0
Zip Compression                 : Deflated
Zip Modify Date                 : 2025:02:26 15:56:48
Zip CRC                         : 0x2a8e3d17
Zip Compressed Size             : 1249907
Zip Uncompressed Size           : 1690811
Zip File Name                   : invoice_document.pdf.bat
```

1. Well, here in the first image, I used the emldump tool to parse and analyze the email files containing headers, body, and attachments. Then I used –s to select which tells to isolate a specific part of the email. Then I used 3 to select index no 3.
2. In the second Image, I used the Exiftool command line tool to read, write, and edit metadata in a wide variety of file types, which are images, videos, PDFs, and audio files etc.



ATT&CK v18 has been released! Check out the blog post or changelog for more information.

TECHNIQUES

- Enterprise
  - Reconnaissance
  - Resource Development
  - Initial Access
    - Content Injection
    - Drive-by Compromise
    - Exploit Public-Facing Application
    - External Remote Services
    - Hardware Additions
    - **Phishing**
    - Replication Through Removable Media
    - Supply Chain Compromise
    - Trusted Relationship
    - Valid Accounts
    - Wi-Fi Networks
  - Execution

Home > Techniques > Enterprise > Phishing

Phishing

Sub-techniques (4)

ID	Name
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.003	Spearphishing via Service
T1566.004	Spearphishing Voice

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., Email Hiding Rules).[1][2]

ID: T1566

Sub-techniques: T1566.001, T1566.002, T1566.003, T1566.004

Tactic: Initial Access

Platforms: Identity Provider, Linux, Office Suite, SaaS, Windows, macOS

Contributors: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaidenberg, @ohad_mz; Philip Winther; Scott Cook, Capital One

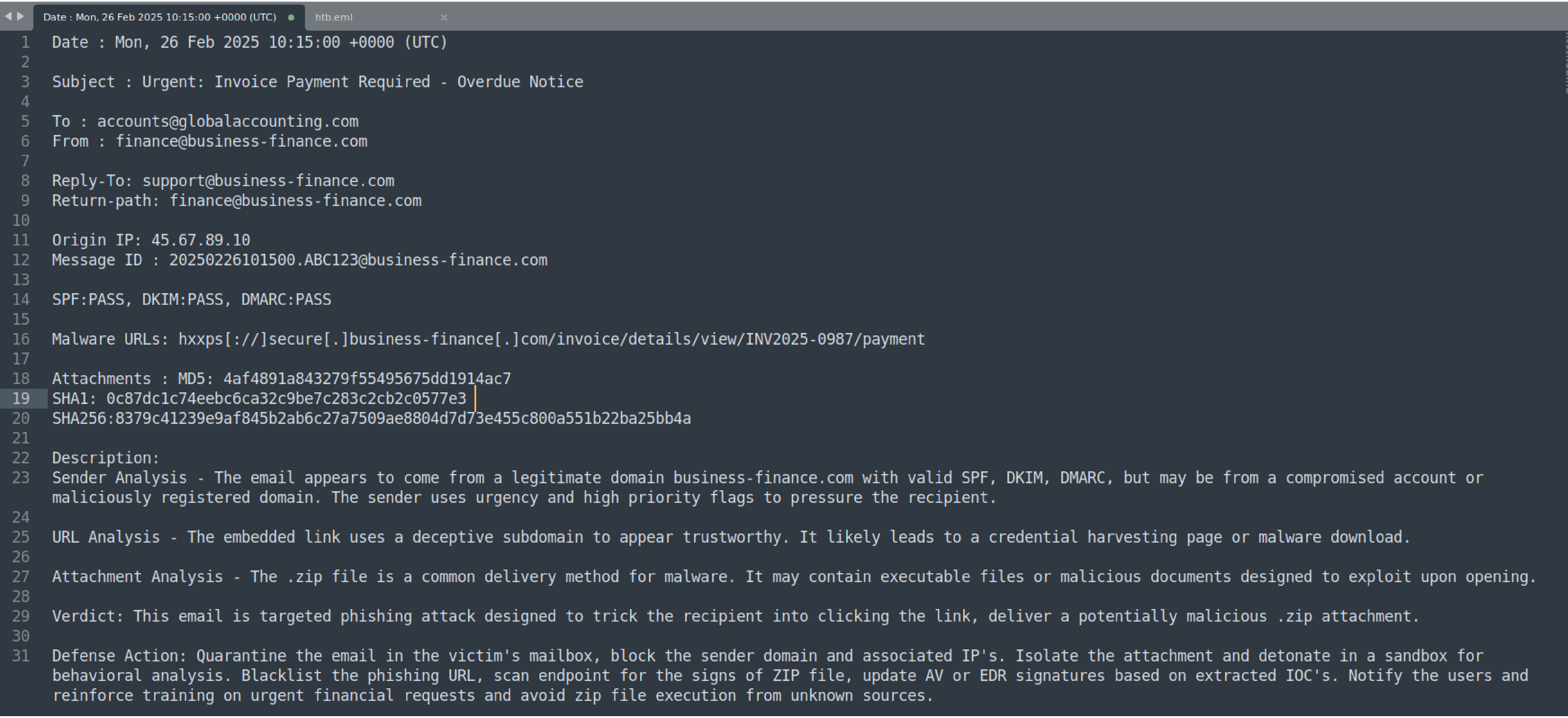
Version: 2.7

Created: 02 March 2020

Last Modified: 24 October 2025

Version Permalink

What Mitre Att&ck techniques are associated with this attack?
MITRE | ATT&CK > Techniques > Enterprise > Initial access > Phishing > Spearphishing attachment.



```
Date : Mon, 26 Feb 2025 10:15:00 +0000 (UTC)

Subject : Urgent: Invoice Payment Required - Overdue Notice

To : accounts@globalaccounting.com
From : finance@business-finance.com

Reply-To: support@business-finance.com
Return-path: finance@business-finance.com

Origin IP: 45.67.89.10
Message ID : 20250226101500.ABC123@business-finance.com

SPF:PASS, DKIM:PASS, DMARC:PASS

Malware URLs: hxxps[://]secure[.]business-finance[.]com/invoice/details/view/INV2025-0987/payment

Attachments : MD5: 4af4891a843279f55495675dd1914ac7
SHA1: 0c87dc1c74eebc6ca32c9be7c283c2cb2c0577e3
SHA256:8379c41239e9af845b2ab6c27a7509ae8804d7d73e455c800a551b22ba25bb4a

Description:
Sender Analysis - The email appears to come from a legitimate domain business-finance.com with valid SPF, DKIM, DMARC, but may be from a compromised account or maliciously registered domain. The sender uses urgency and high priority flags to pressure the recipient.

URL Analysis - The embedded link uses a deceptive subdomain to appear trustworthy. It likely leads to a credential harvesting page or malware download.

Attachment Analysis - The .zip file is a common delivery method for malware. It may contain executable files or malicious documents designed to exploit upon opening.

Verdict: This email is targeted phishing attack designed to trick the recipient into clicking the link, deliver a potentially malicious .zip attachment.

Defense Action: Quarantine the email in the victim's mailbox, block the sender domain and associated IP's. Isolate the attachment and detonate in a sandbox for behavioral analysis. Blacklist the phishing URL, scan endpoint for the signs of ZIP file, update AV or EDR signatures based on extracted IOC's. Notify the users and reinforce training on urgent financial requests and avoid zip file execution from unknown sources.
```

DOCUMENTATION OF EMAIL ANALYSIS