PHISHING EMAIL ANALYSIS REPORT

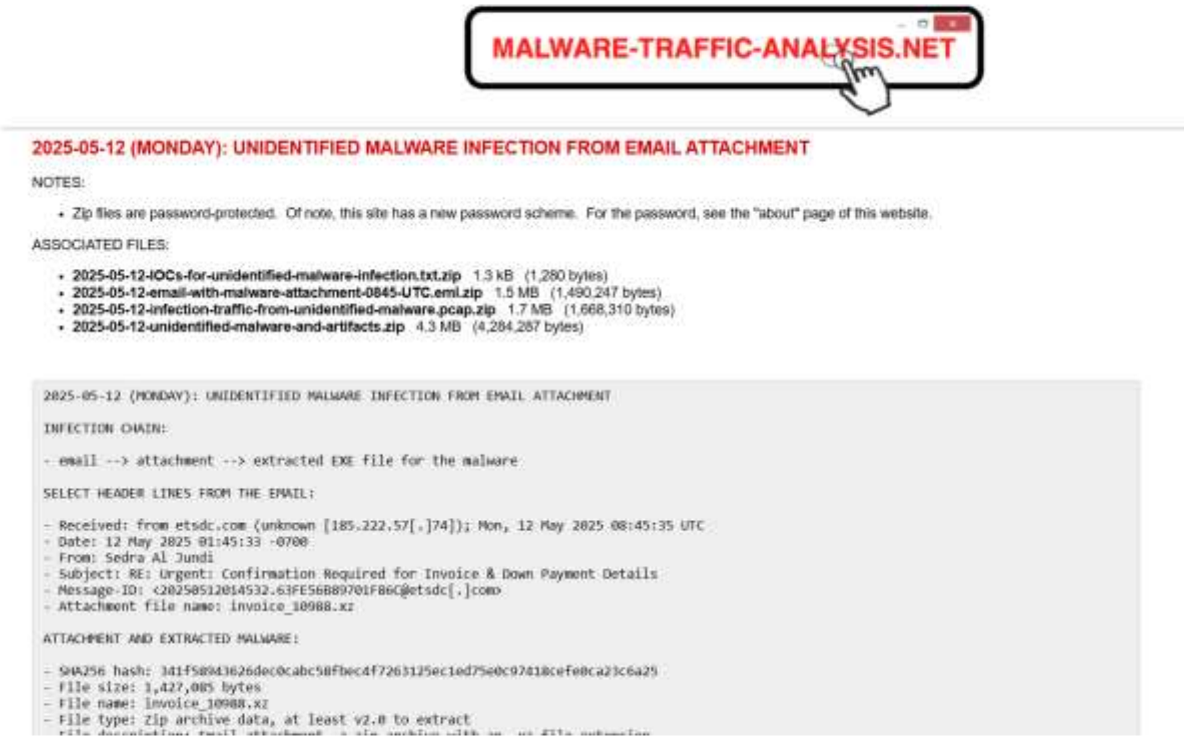
Objective : Identify phishing characteristics in a suspicious email sample.

Tools used :

1. Email client **(Thunderbird email)**
2. free online header analyser **(MXToolbox)**

Email details :

- **Subject : RE :** Urgent confirmation Required for invoice & Down Payment Details
- **Sender Name :** Sedra Al Jundi
- **Sender Email :** cert@etsdc.com
- **Date :** 12 May 2025
- **Attachment :** invoice_10988.xz



2025-05-12 (MONDAY): UNIDENTIFIED MALWARE INFECTION FROM EMAIL ATTACHMENT

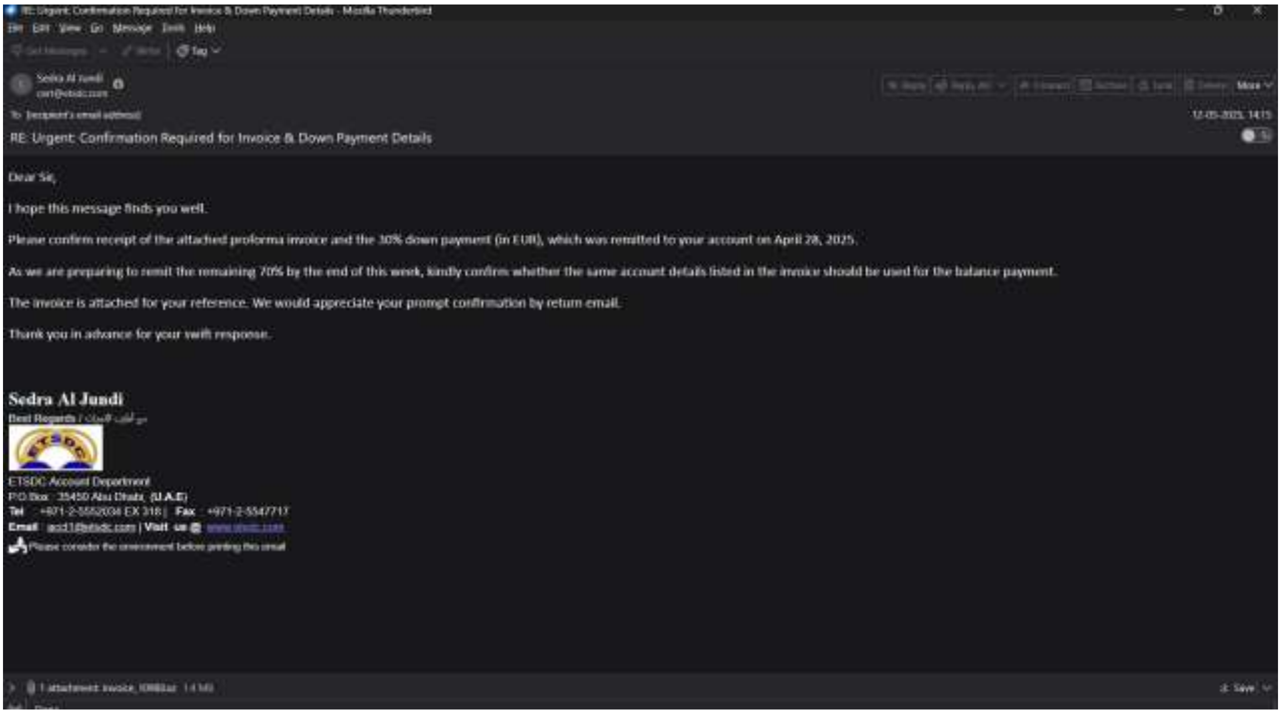
NOTES:

- Zip files are password-protected. Of note, this site has a new password scheme. For the password, see the "about" page of this website.

ASSOCIATED FILES:

- **2025-05-12-IOCs-for-unidentified-malware-infection.txt.zip** 1.3 kB (1,280 bytes)
- **2025-05-12-email-with-malware-attachment-0845-UTC.eml.zip** 1.5 MB (1,490,247 bytes)
- **2025-05-12-infection-traffic-from-unidentified-malware.pcap.zip** 1.7 MB (1,668,310 bytes)
- **2025-05-12-unidentified-malware-and-artifacts.zip** 4.3 MB (4,284,287 bytes)

```
2025-05-12 (MONDAY): UNIDENTIFIED MALWARE INFECTION FROM EMAIL ATTACHMENT

INFECTION CHAIN:

- email --> attachment --> extracted EXE file for the malware

SELECT HEADER LINES FROM THE EMAIL:

- Received: from etsdc.com (unknown [185.222.57[.]74]); Mon, 12 May 2025 08:45:35 UTC
- Date: 12 May 2025 01:45:33 -0700
- From: Sedra Al Jundi
- Subject: RE: Urgent: Confirmation Required for Invoice & Down Payment Details
- Message-ID: <20250512014532.63FE56B89701F86C@etsdc[.]com>
- Attachment file name: invoice_10988.xz

ATTACHMENT AND EXTRACTED MALWARE:

- SHA256 hash: 341f58943626dec0cabc58fbec4f7263125ec1ed75e0c97418cefe0ca23c6a25
- File size: 1,427,085 bytes
- File name: invoice_10988.xz
- File type: Zip archive data, at least v2.0 to extract
- File description: Email attachment, a zip archive with an .xz file extension
```


RE: Urgent: Confirmation Required for Invoice & Down Payment Details - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More
Save

Sedra Al Jundi
cert@etsdc.com

To: [recipient's email address]

12-05-2025, 14:15

RE: Urgent: Confirmation Required for Invoice & Down Payment Details

Dear Sir,

I hope this message finds you well.

Please confirm receipt of the attached proforma invoice and the 30% down payment (in EUR), which was remitted to your account on April 28, 2025.

As we are preparing to remit the remaining 70% by the end of this week, kindly confirm whether the same account details listed in the invoice should be used for the balance payment.

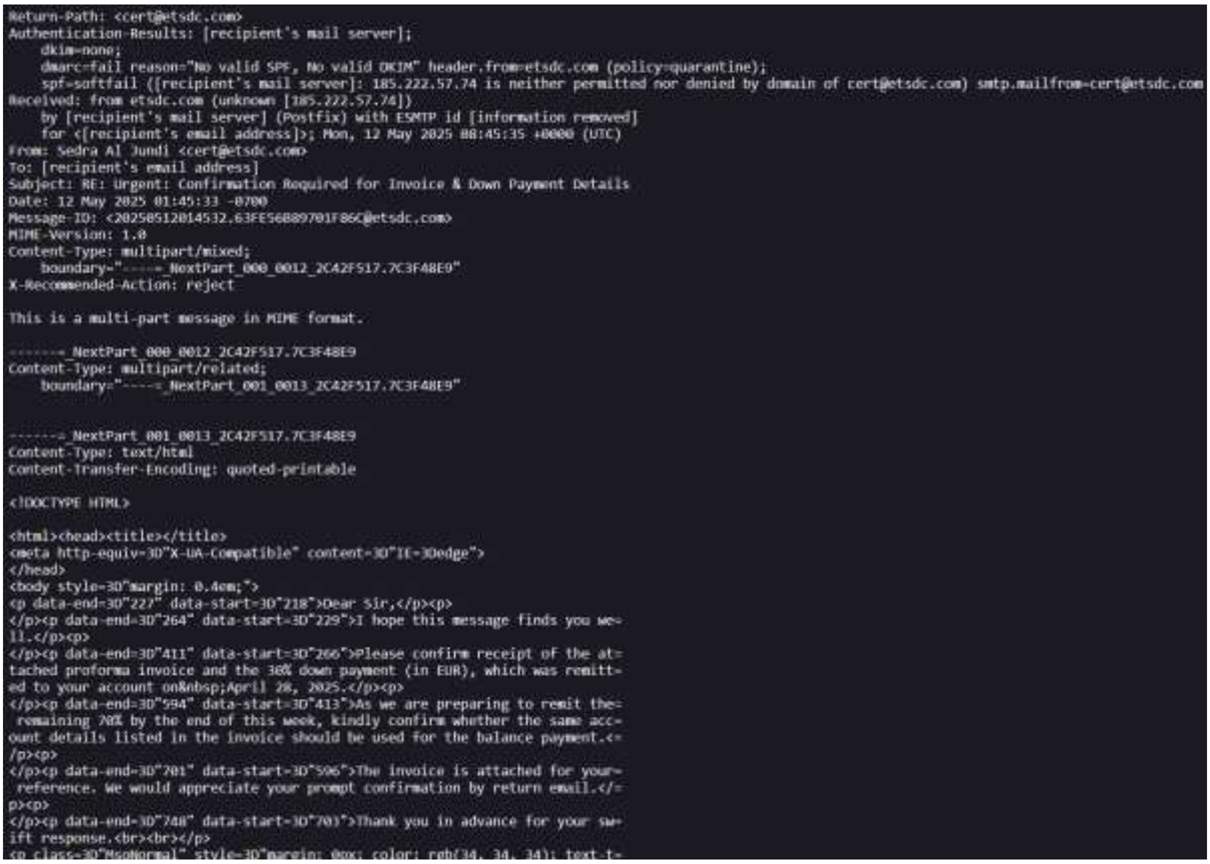
The invoice is attached for your reference. We would appreciate your prompt confirmation by return email.

Thank you in advance for your swift response.

Sedra Al Jundi
Best Regards / مع أطيب التحيات

ETSDC Account Department
P.O.Box : 35450 Abu Dhabi, (U.A.E)
Tel : +971-2-5552034 EX 318 | **Fax** : +971-2-5547717
Email : acct1@etsdc.com | **Visit us @** www.etsdc.com
Please consider the environment before printing this email

1 attachment: invoice_1088.iso 1.4 MB



```
Return-Path: <cert@etsdc.com>
Authentication-Results: [recipient's mail server];
    dkim=none;
    dmarc=fail reason="No valid SPF, No valid DKIM" header.from=etsdc.com (policy=quarantine);
    spf=softfail ([recipient's mail server]: 185.222.57.74 is neither permitted nor denied by domain of cert@etsdc.com) smtp.mailfrom=cert@etsdc.com
Received: from etsdc.com (unknown [185.222.57.74])
    by [recipient's mail server] (Postfix) with ESMTP id [information removed]
    for <[recipient's email address]>; Mon, 12 May 2025 08:45:35 +0000 (UTC)
From: Sedra Al Jundi <cert@etsdc.com>
To: [recipient's email address]
Subject: RE: Urgent: Confirmation Required for Invoice & Down Payment Details
Date: 12 May 2025 01:45:33 -0700
Message-ID: <20250512014532.63FE56B89701F86C@etsdc.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_0012_2C42F517.7C3F48E9"
X-Recommended-Action: reject

This is a multi-part message in MIME format.

------=_NextPart_000_0012_2C42F517.7C3F48E9
Content-Type: multipart/related;
    boundary="----=_NextPart_001_0013_2C42F517.7C3F48E9"


------=_NextPart_001_0013_2C42F517.7C3F48E9
Content-Type: text/html
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML>

<html><head><title></title>
<meta http-equiv=3D"X-UA-Compatible" content=3D"IE=3Dedge">
</head>
<body style=3D"margin: 0.4em;">
<p data-end=3D"227" data-start=3D"218">Dear Sir,</p><p>
</p><p data-end=3D"264" data-start=3D"229">I hope this message finds you we=
ll.</p><p>
</p><p data-end=3D"411" data-start=3D"266">Please confirm receipt of the at=
tached proforma invoice and the 30% down payment (in EUR), which was remitt=
ed to your account on&nbsp;April 28, 2025.</p><p>
</p><p data-end=3D"594" data-start=3D"413">As we are preparing to remit the=
 remaining 70% by the end of this week, kindly confirm whether the same acc=
ount details listed in the invoice should be used for the balance payment.<=
/p><p>
</p><p data-end=3D"701" data-start=3D"596">The invoice is attached for your=
 reference. We would appreciate your prompt confirmation by return email.</=
p><p>
</p><p data-end=3D"748" data-start=3D"703">Thank you in advance for your sw=
ift response.<br><br></p>
<p class=3D"MsoNormal" style=3D"margin: 0px; color: rgb(34, 34, 34); text-t=
```

Phishing Indicators Identified in Email :

- **Urgency and Pressure from sender :**

The subject and body uses urgent language such as “Urgent Confirmation Required ….”, “As we are preparing…… by the end of this week”.
Phishing use urgent language to trick the users into acting without thinking.

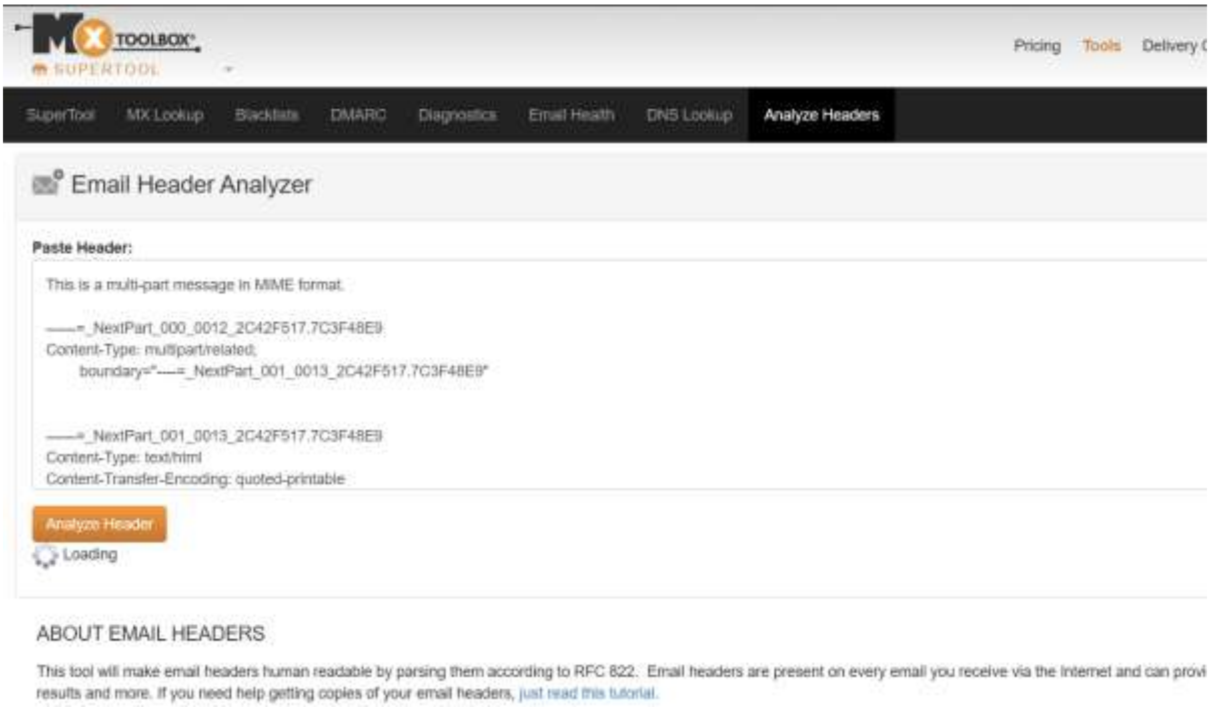
- **Suspicious Attachment :**
  There is an attachment : invoice_10988.xz
  The format .xz is a compressed archieve – not a common invoice format and used often to bypass email filters.

- **Greeting :**
  The email starts with : “Dear Sir,”
  Here, no name is used – this is common in mass phishing where attackers don’t know your name.

- **Sender email Address :**
  The Sender email address does look legal but it can be forged that’s why it is important to check the header of the email.

- **Use of Formal Language :**
  Sentence like : “We would appreciate your prompt confirmation by return email.”
  This type of language is used to sound official which are used commonly in phishing mails.

Header Analysis



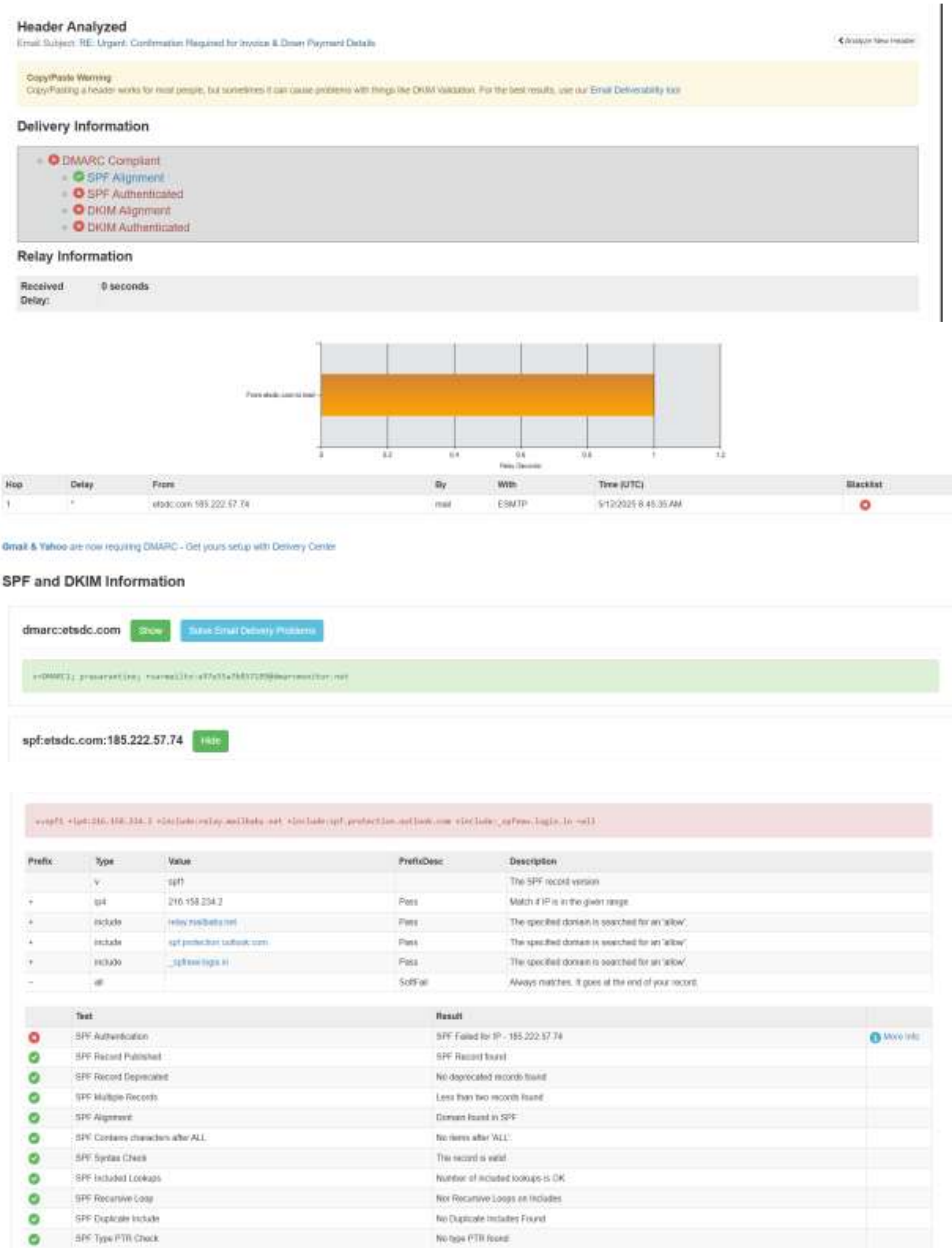
Email Header Analyzer

Paste Header:

```
This is a multi-part message in MIME format.

------=_NextPart_000_0012_2C42F517.7C3F48E9
Content-Type: multipart/related;
	boundary="----=_NextPart_001_0013_2C42F517.7C3F48E9"


------=_NextPart_001_0013_2C42F517.7C3F48E9
Content-Type: text/html
Content-Transfer-Encoding: quoted-printable
```

ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provi
results and more. If you need help getting copies of your email headers, just read this tutorial.



Header Analyzed

Email Subject: RE: Urgent: Confirmation Required for Invoice & Down Payment Details

Copy/Paste Warning
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our Email Deliverability tool

Delivery Information

- ✖ DMARC Compliant
  - ✓ SPF Alignment
  - ✖ SPF Authenticated
  - ✖ DKIM Alignment
  - ✖ DKIM Authenticated

Relay Information

Received Delay:	0 seconds

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	etsdc.com 185.222.57.74	mail	ESMTP	5/12/2025 8:45:35 AM	✖

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

SPF and DKIM Information

dmarc:etsdc.com

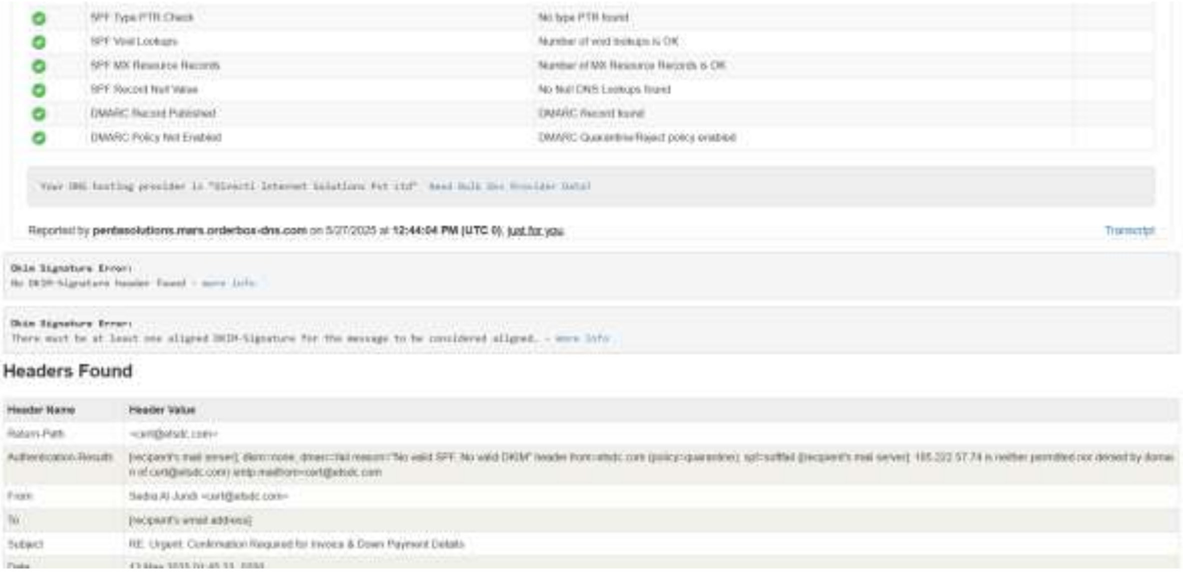
```
v=DMARC1; p=quarantine; rua=mailto:a97a55a7b8572f98@dmarcmonitor.net
```

spf:etsdc.com:185.222.57.74

```
v=spf1 +ip4:216.158.234.2 +include:relay.mailbaby.net +include:spf.protection.outlook.com +include:_spfnew.logix.in ~all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	ip4	216.158.234.2	Pass	Match if IP is in the given range.
+	include	relay.mailbaby.net	Pass	The specified domain is searched for an 'allow'.
+	include	spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'.
+	include	_spfnew.logix.in	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

	Test	Result	
✖	SPF Authentication	SPF Failed for IP - 185.222.57.74	ℹ More Info
✓	SPF Record Published	SPF Record found	
✓	SPF Record Deprecated	No deprecated records found	
✓	SPF Multiple Records	Less than two records found	
✓	SPF Alignment	Domain found in SPF	
✓	SPF Contains characters after ALL	No items after 'ALL'.	
✓	SPF Syntax Check	The record is valid	
✓	SPF Included Lookups	Number of included lookups is OK	
✓	SPF Recursive Loop	No Recursive Loops on Includes	
✓	SPF Duplicate Include	No Duplicate Includes Found	
✓	SPF Type PTR Check	No type PTR found	



✓	SPF Type PTR Check	No type PTR found
✓	SPF Void Lookups	Number of void lookups is OK
✓	SPF MX Resource Records	Number of MX Resource Records is OK
✓	SPF Record Null Value	No Null DNS Lookups found
✓	DMARC Record Published	DMARC Record found
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

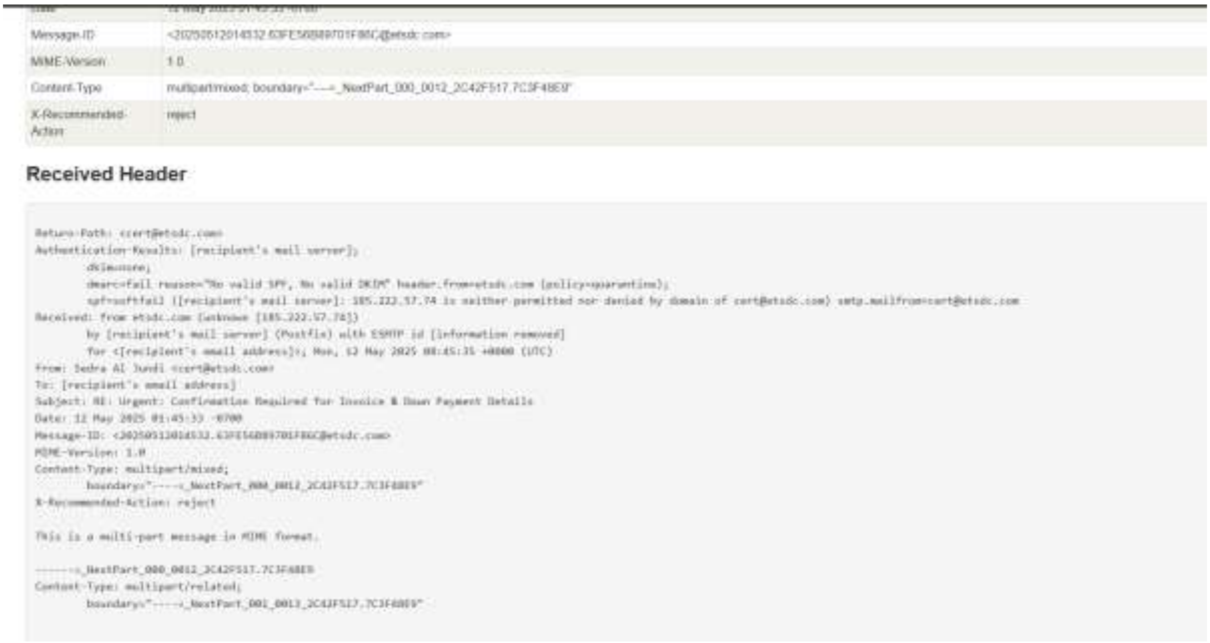
```
Your DNS hosting provider is "Directi Internet Solutions Pvt Ltd" Need Bulk Dns Provider Data?
```

Reported by **pentasolutions.mars.orderbox-dns.com** on 5/27/2025 at **12:44:04 PM (UTC 0)**, just for you. Transcript

```
Dkim Signature Error:
No DKIM-Signature header found - more info
```

```
Dkim Signature Error:
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info
```

Headers Found



Header Name	Header Value
Return-Path	<cert@etsdc.com>
Authentication-Results	[recipient's mail server]; dkim=none; dmarc=fail reason="No valid SPF, No valid DKIM" header.from=etsdc.com (policy=quarantine); spf=softfail ([recipient's mail server]: 185.222.57.74 is neither permitted nor denied by domain of cert@etsdc.com) smtp.mailfrom=cert@etsdc.com
From	Sedra Al Jundi <cert@etsdc.com>
To	[recipient's email address]
Subject	RE: Urgent: Confirmation Required for Invoice & Down Payment Details
Date	12 May 2025 01:45:33 -0700
Message-ID	<20250512014532.63FE56B89701F86C@etsdc.com>
MIME-Version	1.0
Content-Type	multipart/mixed; boundary="----=_NextPart_000_0012_2C42F517.7C3F4BE9"
X-Recommended-Action	reject

Received Header

```
Return-Path: <cert@etsdc.com>
Authentication-Results: [recipient's mail server];
        dkim=none;
        dmarc=fail reason="No valid SPF, No valid DKIM" header.from=etsdc.com (policy=quarantine);
        spf=softfail ([recipient's mail server]: 185.222.57.74 is neither permitted nor denied by domain of cert@etsdc.com) smtp.mailfrom=cert@etsdc.com
Received: from etsdc.com (unknown [185.222.57.74])
        by [recipient's mail server] (Postfix) with ESMTP id [information removed]
        for <[recipient's email address]>; Mon, 12 May 2025 08:45:35 +0000 (UTC)
From: Sedra Al Jundi <cert@etsdc.com>
To: [recipient's email address]
Subject: RE: Urgent: Confirmation Required for Invoice & Down Payment Details
Date: 12 May 2025 01:45:33 -0700
Message-ID: <20250512014532.63FE56B89701F86C@etsdc.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0012_2C42F517.7C3F4BE9"
X-Recommended-Action: reject

This is a multi-part message in MIME format.

------=_NextPart_000_0012_2C42F517.7C3F4BE9
Content-Type: multipart/related;
        boundary="----=_NextPart_001_0013_2C42F517.7C3F4BE9"
```

- **SPF:** Failed – The email was sent from an unauthorized IP (185.222.57.74) not allowed by the etsdc.com domain.
- **DKIM:** Failed – No valid DKIM signature was found, indicating the message could have been altered.
- **DMARC:** Failed – Since both SPF and DKIM failed, DMARC policy marked the message for quarantine.
- **Source IP:** Suspicious and not associated with the official domain; possibly listed in blacklists.
- **Recommended Action:** Reject – The server flagged the message as untrusted.

Conclusion

This email is a **confirmed phishing attempt** delivering malware via a disguised attachment and social engineering tactics. It is crafted to appear like a legitimate financial transaction but fails authentication checks and contains a malicious file.

Recommendations

- Do not open such attachments.
- Always verify the sender via official communication channels.
- Use email security tools to detect spoofing.
- Educate employees about phishing indicators.