SMTP 550 Bounce Email Analysis – Forensic Examination of a Legitimate Non-Delivery Report

Executive Summary

This report provides a detailed forensic analysis of a bounce notification (SMTP error 550 5.4.1) extracted from a .eml file during email forensics training. The objective is to validate the legitimacy of the message and demonstrate an effective methodology for distinguishing genuine system notifications from malicious or spoofed emails, following international cybersecurity reporting standards.

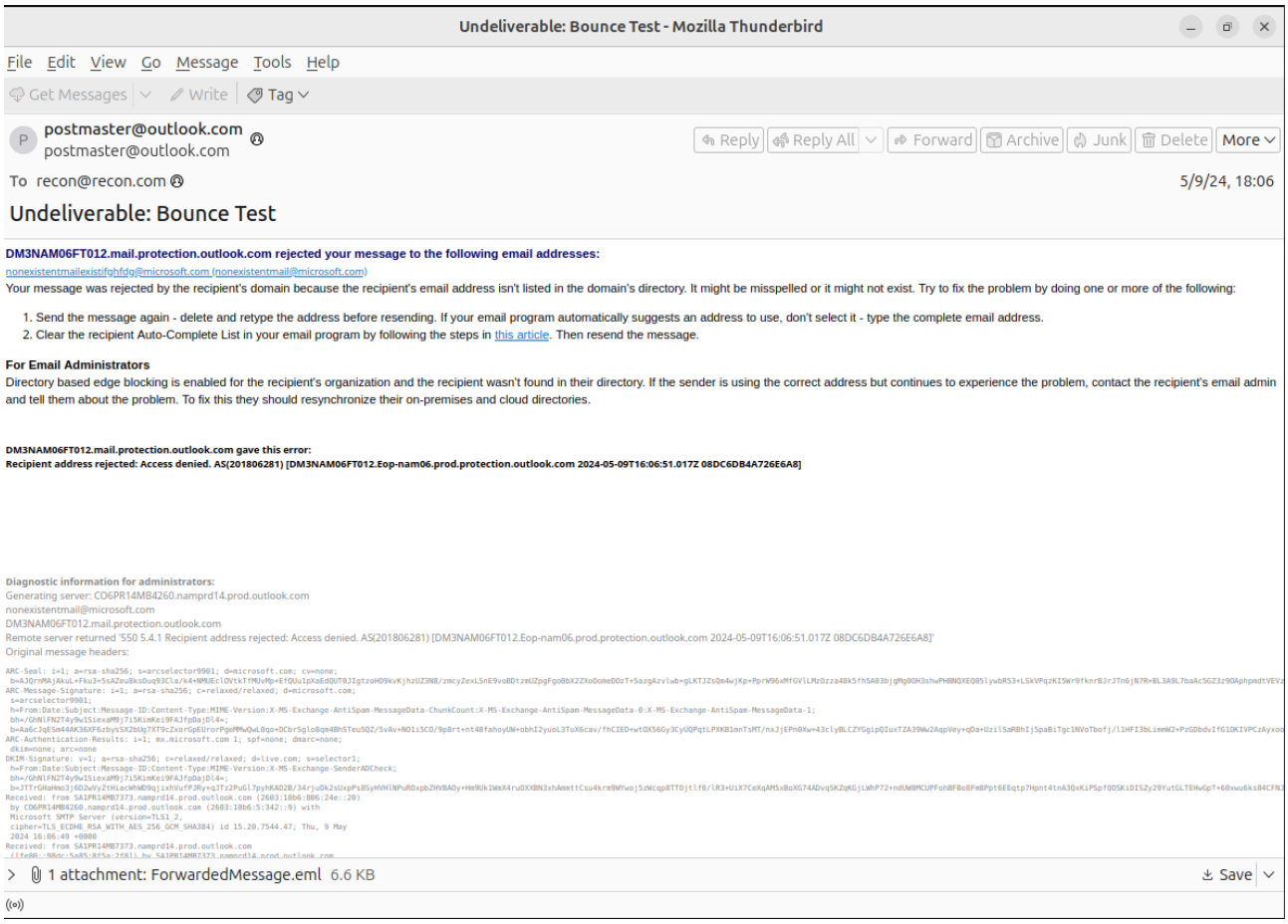
1. Introduction

A non-delivery report (NDR), or bounce message, is an automated response generated by mail servers to communicate failed email delivery. Understanding and verifying these notifications is essential for Security Operations Center (SOC) analysts to rule out phishing or infrastructure attacks.

2. Initial Assessment

- The email displays characteristics typical of a system-generated bounce:
    - Sender: Outlook postmaster
    - Recipient: Invalid Microsoft address
    - Subject: Standard delivery error
    - Error: SMTP 550 5.4.1 (“Recipient address rejected: Access denied”)
- Visual inspection with Thunderbird and Sublime Text confirms no suspicious attachments, links, or external content.

Image 1: Email opened with Thunderbird/Sublime Text
(Screenshot visually matches described state of the bounced message, with no signs of tampering.)



3. Technical Header Analysis

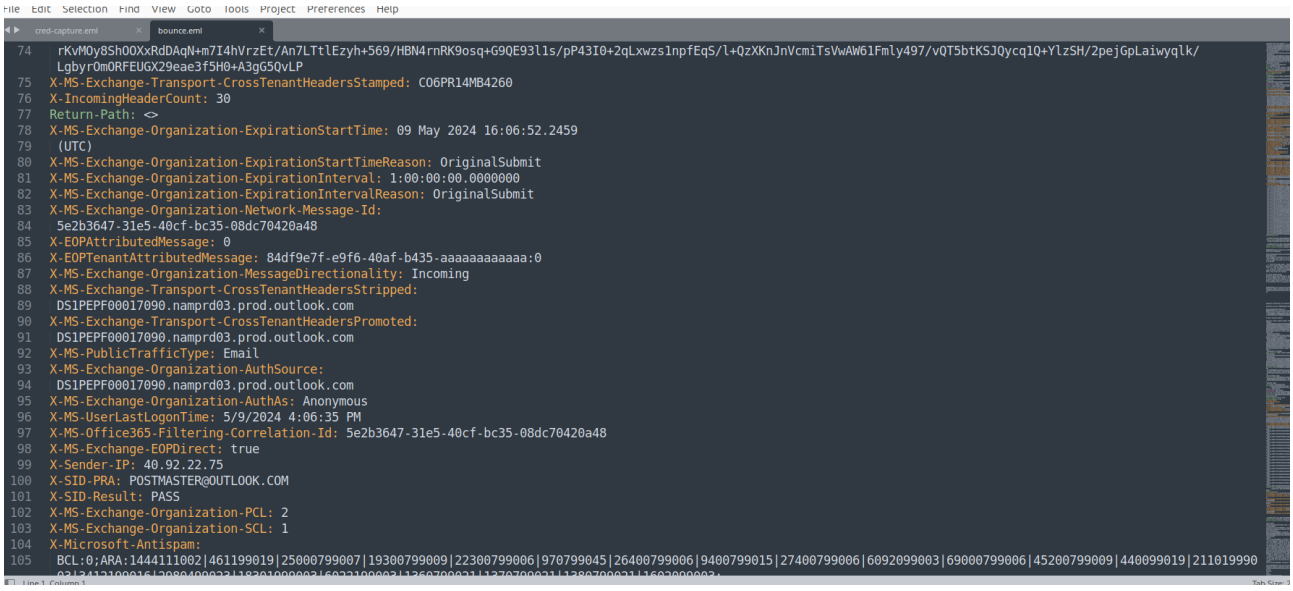
- Full message headers display the expected SMTP elements for a legitimate bounce.
- "From" is the Outlook postmaster; "To" is the invalid recipient; message ID and subject align with genuine delivery reports.
- The ".eml" attachment inside the analyzed email contains a technical copy of the failed message only.

Image 2: Full email headers in Sublime Text
(Visual evidence supports text: no anomalous fields or inconsistencies. Subsequent screenshots highlight timestamps, sender, recipient, subject, message ID, and reply-to — all as expected in valid NDRs.)

```
b=knseatSkCt6Ngox/f8KKWa8nT8w3XpP6VV0SYGN2744vS9veCRlzx5JITI3ib2fccUNKUSYE69xzf8EPyOxPplHQv8Ep+uqzF6XM//iSkwkkkzKlTKvIN/
Pa9H2eaQQpr4YI74NVkfSt+tEIhZSzg1qboxowTKTcBtNzTpApBPKYqAjHqfYdgyl3G1yoGfCcLwzpW0nh8YO7rnzWo8A50wibWIsYxvW8XqNDHqIrezJJcNc2lhgER9gFwSUCqNFz+FN/0ThRkiQ/
erQUGshhnNQxuTFnB35CCa/wfsHJYhJviNLPeWF8a+Z/778EhJMQQF75TQROP+l1QOx4Oc06gw==
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=none; dmarc=none;
 dkim=none; arc=none
From: <postmaster@outlook.com>
To: <recon@recon.com>
Date: Thu, 9 May 2024 16:06:51 +0000
Content-Type: multipart/report; report-type=delivery-status;
  boundary="45fb354b-9146-4bf0-85be-d66260bc1fff"
X-MS-Exchange-Message-Is-Ndr:
Content-Language: en-CA
Message-ID:
 <ae60f018-2d84-4b77-89da-ccb658313095@CO6PR14MB4260.namprd14.prod.outlook.com>
In-Reply-To:
 <SA1PR14MB7373523AD66968D5B363E97AC1E62@SA1PR14MB7373.namprd14.prod.outlook.com>
References:
 <SA1PR14MB7373523AD66968D5B363E97AC1E62@SA1PR14MB7373.namprd14.prod.outlook.com>
Thread-Topic: Bounce Test
Thread-Index: AQHaoirlYykmnTkTKEinqvu+Dbg7IrGPEXha
Subject: Undeliverable: Bounce Test
Auto-Submitted: auto-replied
X-MS-TrafficTypeDiagnostic:
 CO6PR14MB4260:EE_|DS1PEPF00017090:EE_|LV3PR14MB7694:EE_|SA1PR14MB7373:EE_
X-Microsoft-Antispam-Untrusted:
 BCL:0;ARA:14566002|9400799015|6092099003|461199019|3412199016|440099019|1602099003;
X-Microsoft-Antispam-Message-Info-Original:
 KCrXcQnwEZZKpkZMHLsoyLE+dUGuMGD61HA42TIG1u405D0Utb4YTI6cMQGtc30Pf5+qs9ED3mnAo3CUEWjoRWKnNX/jE+mZZx7GC4y34MOmXJ14/ngXoME+KIgIxIARcqMsfTrudfMUbDk6j2d9wzgfW4UT5GcS28bb2S
 IMQLiiH2RIs6jx9kJtfuVsbVc0Xux2ihkDOFGBOZRnMqi8oJYzYDjM0MIuFKcVRC7qmh4aAnzx9yvB9ETtQTQnvh6D8ICG59LEVOeSvDRQV7xL2hc2XdOOHa4Psdll4I5OyCNythdtXxqIZGFb9M4fBaQ9uideypV6PpsL
 Ubs+AVPw1CMNj/X4bVXn3g6MzyO5Cgi2oZhT5KfAktlQpeZndgHRv09tcBGPW/
 HBygFUiKhECIeTapskz1lNv1328Ma0bbURaJUD3tjeKEVlSLcK1PGbsadHqzk6JrSlgdJBsMMN4TgZMENDVpjNcVeYdXY6MC98S9owm8SigdV+DF7OdAvXp8VqPcAjwA+qcbsMGW/
 F30XSJUuaeN+g2dupNpxyNI2zSj9dAIkQRuehtSIL4CylGAmvyG/bNhT+S00rhyXwyLgCX0taSxO7Ov+n8bKH8O+tIAR3Hc8t/SevSKjkjq5+zmOWKy/OsLlz/S2veoRzJ+l+MaCRyB+/40uhIcYZAwj378JohW3tAYO5S
 ozP5Ly7l03oGNX2ZvoUgNJo9AyllJA9DstL267MDBvlJ7yQXCvlQnHT054QH6eNFpXlmAGQ1oBTbAfJRAKUrex365Lr25W18sT+GxauACmI5ee+5ov6zmodMPCzO3UWVFq1vzPiXqR3g5USSnvdwjFtSfYwW6dqOpzQhSC
```

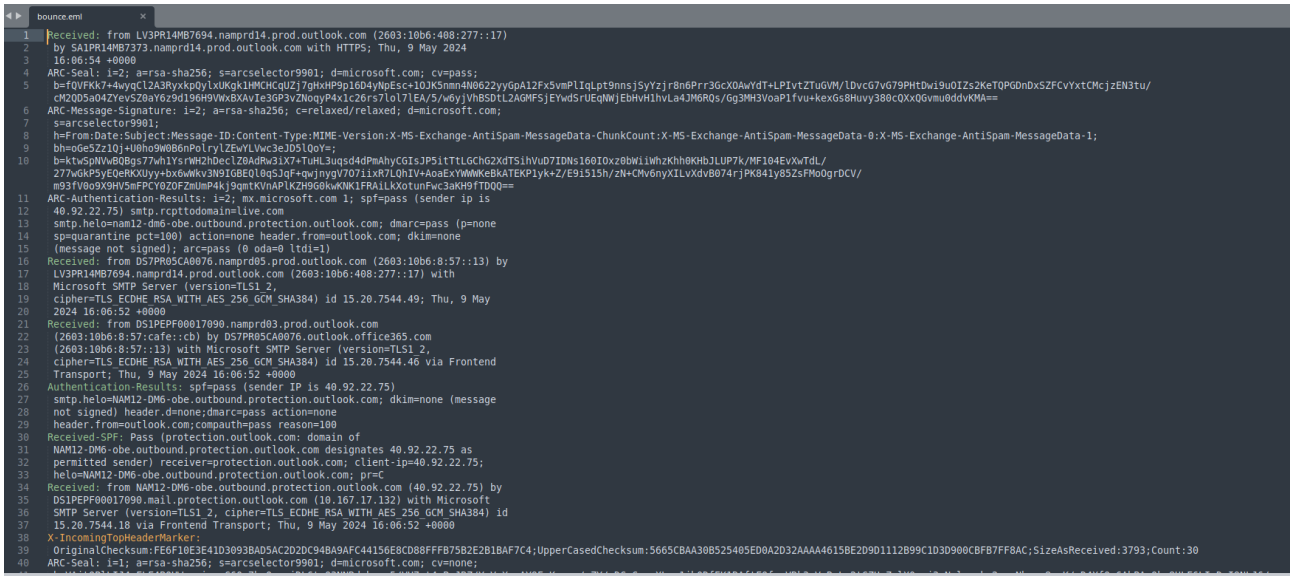
4. Return Path and IP Trace

- The "Return-Path" header for this bounce notification is empty (<>), as mandated by the SMTP standard. This is expected in legitimate non-delivery reports and prevents mail loops. The absence of a domain in the Return-Path is not an indicator of spoofing or malice, but rather confirms proper handling by the Microsoft mail server.
- The "X sender IP" field reveals IP address 40.92.22.75.
- Reverse IP lookup with DomainTools indicates the address is registered with Microsoft Corporation and part of the Outlook outbound mail server range.



5. Received Header Review

- By examining "Received" fields (bottom-up), the earliest handoff is from a Microsoft mail infrastructure server, with no evidence of third-party hops.
- The message passed only through trusted Microsoft-operated servers, consistent with authentic bounce messages.



6. Conclusion

Based on:

- Header field consistency
- IP ownership and message routing validation
- Absence of malicious indicators in both message body and attachments

This bounce email is confirmed as a legitimate non-delivery notification from Microsoft infrastructure.
No evidence of spoofing, phishing, or attempt at payload delivery was detected.