Cybersecurity

Activity File

Module 9 Day 2

Activity File: Email Networking

In this activity, you will continue to play the role of a security analyst at Acme Corp.

- Acme Corp's CFO recently received several suspicious emails.
- You must analyze the header records of the suspicious emails and document several data points.

Instructions

VIew the 5 suspicious emails provided below. For each, determine the following data points:

- Delivered-To
- Return-Path
- IP address of source domain
- Message-ID

Open the same suspicious emails provided from the previous activity and complete the following:

- Examine the email headers to determine which of the emails are spoofed and which are legitimate.
- Scan any links using scamadviser.com and document the trustscore.

Answer the following questions:

- An email fails the Received-SPF verification, but was a legitimate email.
    - What does this indicate?
    - What would you recommend to prevent future emails from failing this validation?

Email 1:

- Delivered-To: juliejones@acme.com
- Return-Path: jonathanthomas@microsoft.com
- IP address of source: 40.76.4.15
- Message-ID: 1689837351.2998569.1568044304435@mail.microsoft.com
- Received-SPF: "Pass" on behalf of Microsoft.
- From: Jonathan Thomas jonathanthomas@microsoft.com the email and name match.
- Summary: The records in the header indicate it is safe.

Email 2:

- Delivered-To: juliejones@acme.com
- Return-Path: xzvvvret34344@yahoo.com
- IP address of source: 74.6.130.41
- Message-ID: 1689837351.2998569.1568044304435@mail.yahoo.com
- Received-SPF: "Pass" on behalf of Yahoo.
- From: Michael Smith xzvvvret34344@yahoo.com the name and email do not match and the email looks suspicious.
- Summary: The mismatch of the name makes it likely this is a spoof email.

Email 3:

- Delivered-To: juliejones@acme.com
- Return-Path: timmytom@widgets.com
- IP address of source: 34.86.130.49
- Message-ID: 1gytrdd9837351.987987abs9.1568044304435@mail.widgets.com
- Received-SPF: "Fail" indicates that it is not from an authorized email provider.
- From: Timmy Tom timmytom@widgets.com the name and email match.
- Summary: The failed SPF record usually indicates a spoofed email.

Email 4:

- Delivered-To: juliejones@acme.com
- Return-Path: return@irs.org
- IP address of source: 64.71.74.115
- Message-ID: 404021289698796556000_1102202887875875711 7@jdq.hentersss.com
- Received-SPF: "Fail" indicates that it is not from an authorized email provider for the IRS.
- From: IRS Assistance Programs m1T7pqweeqweD8G@thought.bestwebsitesabc.com—the name and email do not match.

- Summary: The failed SPF record and the obvious mismatch of the from email address is a strong indicator this is a spoofed email.

Email 5:
- Delivered-To: juliejones@acme.com
- Return-Path: billybob@companyA.com
- IP address of source: 209.85.210.51
- Message-ID: CACLG$52234Ygm1FNJZWXQc=dR-cv-jw+KRbRPf455BU6E-Xp_xDEA@mail.gmail.com
- Received-SPF: "Pass" on behalf of CompanyA.
- From: Billy Bob billybob@companyA.com the email and name match.
- Summary: The records in the header indicate it is safe.

An email fails the Received-SPF verification, but was a legitimate email. This most likely indicates that the mail server sending emails on behalf of the domain doesn't have a DNS SPF record. To resolve this, an SPF record should be added with the IP of the mail server sending these emails.

EMAIL 1

Delivered-To: juliejones@acme.com
Received: by 2002:a9d:5544:0:0:0:0:0 with SMTP id h4csp4292866oti;
Mon, 9 Sep 2019 08:51:49 -0700 (PDT)
X-Received: by 2002:ac8:518a:: with SMTP id c10mr10356217qtn.351.1568044309518;
Mon, 09 Sep 2019 08:51:49 -0700 (PDT)
Return-Path: <jonathanthomas@microsoft.com>
Received: from microsoft.com (microsoft.com. [40.76.4.15])
for <juliejones@acme.com>
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Mon, 09 Sep 2019 08:51:49 -0700 (PDT)
Received-SPF: pass (google.com: domain of jonathanthomas@microsoft.com designates 40.76.4.15 as permitted sender) client-ip=40.76.4.15;

To: Julie Jones <juliejones@acme.com>
Message-ID: <1689837351.2998569.1568044304435@mail.microsoft.com>
Subject: Update Notification from Microsoft
From: Jonathan Thomas <jonathanthomas@microsoft.com>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="----=_Part_2998568_1954224285.1568044304435"
References: <1689837351.2998569.1568044304435.ref@mail.microsoft.com>
X-Mailer: WebService/1.1.14303 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Length: 560

------=_Part_2998568_1954224285.1568044304435
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

Dear Julie,

This is just a friendly reminder from Microsoft, that your license for MS Office is expiring soon. Please visit microsoft.com to update your license.

Thanks,
Jonathan Thomas
Client Support
Microsoft

EMAIL 2

Delivered-To: juliejones@acme.com
Received: by 2002:a9d:5544:0:0:0:0:0 with SMTP id gytre34329466oti;
Mon, 9 Sep 2019 08:53:49 -0700 (PDT)
X-Received: by 2002:ac8:538a:: with SMTP id c10mr10356217qtn.351.1568044309518;
Mon, 09 Sep 2019 08:53:49 -0700 (PDT)
Return-Path: <xzvvvret34344@yahoo.com>
Received: from sonic308-2.consmr.mail.bf2.yahoo.com (sonic308-2.consmr.mail.bf2.yahoo.com. [74.6.130.41])
by mx.google.com with ESMTPS id x24si2689288qki.191.2019.09.09.08.51.49
for <juliejones@acme.com>
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Mon, 09 Sep 2019 08:53:49 -0700 (PDT)
Received-SPF: pass (google.com: domain of xzvvvret34344@yahoo.com designates 74.6.130.41 as permitted sender) client-ip=74.6.130.41;

To: Julie Jones <juliejones@acme.com>
Message-ID: <1689837351.2998569.1568044304435@mail.yahoo.com>
Subject: test email
From: Michael Smith <xzvvvret34344@yahoo.com>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="----=_Part_2998568_1954224285.1568044304435"
References: <1689837351.2998569.1568044304435.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.14303 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Length: 560

------=_Part_2998568_1954224285.1568044304435
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

Hello,

This is Michael Smith from Widgets.com. You are overdue on your balance of $6434.43. Please submit your payment right away to avoid severe penalties.

Click the following link to submit your payment here ASAP!

www.makepaymentnowplease.com

Thank you,
Michael Smith

EMAIL 3

Delivered-To: juliejones@acme.com
Received: by 2002:a9d:4e8e:0:0:0:0:0 with SMTP id v14csp1030449otk;
Mon, 9 Sep 2019 08:57:51 -0700 (PDT)
X-Received: by 2002:ac8:578a:: with SMTP id c10mr10356217qtn.351.1568044309518;
Mon, 09 Sep 2019 08:57:51 -0700 (PDT)
Return-Path: <timmytom@widgets.com>
Received: from spammers.com (spammers.com. [34.86.130.49])
by mx.google.com with ESMTPS id x24si2689288qki.191.2019.09.09.08.51.49
for <juliejones@acme.com>
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Mon, 09 Sep 2019 08:51:49 -0700 (PDT)
Received-SPF: fail (google.com: domain of timmytom@widgets.com does not designate 34.86.130.49 as permitted sender) client-ip=34.86.130.49 ;

To: Julie Jones <juliejones@acme.com>
Message-ID: <1gytrdd9837351.987987abs9.1568044304435@mail.widgets.com>
Subject: Wire Request
From: Timmy Tom <timmytom@widgets.com>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="----=_Part_2998568_1954224285.1568044304435"
References: <1689837351.2998569.1568044304435.ref@mail.widgets.com>
X-Mailer: WebService/1.1.14303 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Length: 560

------=_Part_2998568_1954224285.1568044304435
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

Hi Julie,

Just a reminder to please send the wirepayment out for $10,000 as soon as possible to the following addresss:

Wire ABA# 34252345356564645
Band Account number: 24590003344333

Thank you,
Timmy Tom

EMAIL 4

Delivered-To: juliejones@acme.com
Received: by 2002:a67:7a8b:0:0:0:0:0 with SMTP id v139879879vsc;
Mon, 9 Sep 2019 19:23:37 -0700 (PDT)
X-Received: by 2002:a67:c581:: with SMTP id h1mr8879576vsk.239.1567909417816;
Mon, 09 Sep 2019 19:23:37 -0700 (PDT)
Return-Path: <return@irs.org>
Received: from domain.com (thought.bestwebsitesabc.com. [64.71.74.115])
by mx.google.com with ESMTP id g9si608412vsa.17.2019.09.07.19.23.37
for <juliejones@acme.com>;
Sat, 07 Sep 2019 19:23:37 -0700 (PDT)
Received-SPF: fail (google.com: domain of return@irs.org does not designate 64.71.74.115 as permitted sender) client-ip=64.71.74.115;
subject: : FROM THE IRS!!!
From: IRS Assistance Programs <m1T7pqweeqweD8G@thought.bestwebsitesabc.com>
To: mae.andrews@gmail22.com, smae.andrews2@gmail22.com,juliejones@acme.com, juliejones1@acme.com, juliejones2@acme.com
Message-ID: <404021289698796556000_1102202887875857117@jdq.hentersss.com>
content-Type: text/html;
Content-Disposition: inline
Date: Mon, 09 Sep 2019 22:23:37 -0400 (EDT)
Content-Length: 560

------=_Part_2998568_1954224285.1568044304435
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

Dear IRS Customer,

**This is the IRS and we know you owe the IRS a large sum of funds. This is a one time opportunity to make a payment to the IRS to cancel
all your debt. Please send 5 bitcoins to the following address, paybybitcoin.com.**

**Thank you,
Your friends at the IRS**

EMAIL 5

Delivered-To: juliejones@acme.com
Return-Path: <billybob@companyA.com>
Received-SPF: pass (domain of companyA.com designates 209.85.210.51 as permitted sender)
X-Originating-IP: [209.85.210.51]
Received: from 10.213.171.100 (EHLO mail-ot1-f51.google.com) (209.85.210.51)
  by mta4419.mail.gq1.acme.com with SMTPS; Mon, 09 Sep 2019 17:36:31 +0000
Received: by mail-ot1-f51.google.com with SMTP id t6so18234234otp.2
        for <julie.jones@acme.com>; Mon, 09 Sep 2019 10:36:30 -0700 (PDT)
 Mon, 09 Sep 2019 10:36:30 -0700 (PDT)
MIME-Version: 1.0
From: Billy Bob <billybob@companyA.com>
Date: Mon, 9 Sep 2019 13:36:21 -0400
Message-ID: <CACLG$52234Ygm1FNJZWXQc=dR-cv-jw+KRbRPf455BU6E-Xp_xDEA@mail.gmail.com>
Subject: Can we have a meeting tomorrow at noon?
To: julie.jones@acme.com
Content-Type: multipart/alternative; boundary="000000000000707752059223acd"
Content-Length: 627

--000000000000707752059223acd
Content-Type: text/plain; charset="UTF-8"

Hi Julie,

Was hoping we could meet for a meeting tomorrow at noon to discuss the merger and acquisition?

Thank you,
Billy Bob

--