Email Analysis (Phishing)

Project Description

In this project, I will be analyzing an email given from a scenario provided by the Blue Team Labs website.

Software and Tools

- Kali Linux VM
- CyberChef
- Gary Kessler Signature Files
- HxD
- Square X
- Exiftool

Walkthrough

First, I downloaded the email file given by the scenario. Then, I opened it using Notepad++. The following image shows a fraction of the email.

```
Return-Path: <billjobs@microapple.com>
Received: from localhost (emkei.cz. [93.99.104.210])
        by mx.google.com with ESMTPS id s16si170171wmj.176.2021.01.25.22.41.18
        for <themajoronearth@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-CHACHA20-POLY1305 bits=256/256);
        Mon, 25 Jan 2021 22:41:18 -0800 (PST)
Received-SPF: fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender)
Authentication-Results: mx.google.com;
        spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) sm
Received: by localhost (Postfix, from userid 33)
    id 1993E221F8; Tue, 26 Jan 2021 01:41:18 -0500 (EST)
To: themajoronearth@gmail.com
Subject: A Hope to CoCanDa
From: "Bill" <billjobs@microapple.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: billjobs@microapple.com
Reply-To: negeja3921@pashter.com
MIME-version: 1.0
Content-Type: multipart/mixed; boundary=BOUND_600FB98E0DCEE8.49207210
Message-Id: <20210126064118.1993E221F8@localhost>
Date: Tue, 26 Jan 2021 01:41:18 -0500 (EST)
```

Based on the image, I can already see that the sender used *emkei,* a fake mailer*,* as the email service. Also, there is a discrepancy with the sender email address (<mark>billjobs@microapple.com</mark>) and the reply-to email address (<mark>negeja3921@pashter.com</mark>). Another observation is that the SPF authentication protocol failed to authenticate the sender. As I continued looking at the email, I found a message encoded with base64 format as shown in the following image.

```
--BOUND_600FB98E0DCEE8.49207210
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64

SGkgVGhlTWFqb3JPbkVhcnRoLAoKVGhlIGFiZHVjdGVkIENvQ2FuRGlhbnMgYXJlIHdpdGggbWUg
aW5jbHVkaW5nIHRoZSBQcmVzaWRlbnTigJzIGRhdWdodGVyLiBEb250IHdvcnJ5LiBUaGV5IGFy
ZSBzYWZlIGluIGEgc2VjcmV0IGxvY2F0aW9uLgpTZW5kIG1lIDEgQmlsbGlvbiBDb0NhbkRz8J+k
kSBpbiBjYXNo8J+SuCB3aXRoIGEgc3BhY2VzaGlw8J+agCBhbmQgbXkgYXV0b25vbW91cyBib3Rz
IHdpbGwgc2FmZWx5IGJyaW5nIGJhY2sgeW91ciBjaXRpemVucy4KCkkgaGVhcmQgdGhhdCBDb0Nh
bkRpYW5zIGhhdmUgdGhlIGJlc3QgYnJhaW5zIGluIHRoZSBVbml2ZXJzZS4gU29sdmUgdGhlIHB1
enpsZSBJIHNlbnQgYXMgYW4gYXR0YWNobWVudCBmb3IgdGhlIG5leHQgc3RlcHMuCgpJ4oCZbSBh
cHByb3hpbWF0ZWx5IDEyLjggbGlnaHQgbWludXRlcyBhd2F5IGZyb20gdGhlIHN1biBhbmQgbXkg
YWR2aWNlIGZvciB0aGUgcHV6emxlIGlzIAoK4oCcRG9uJ3QgVHJ1c3QgWW91ciBFeWVz4oCdCgpM
b2zwn5iCCgpTZWUgeW91IE1ham9yLiBXYWl0aW5nIGZvciB0aGUgQ2Fzc3NoaGho8J+SsA==
```

Since the message was encoded in base64 format, I proceeded to use CyberChef to decode it. After I copied the message to CyberChef, the real message was revealed as shown in the image below.

Hi TheMajorOnEarth,

The abducted CoCanDians are with me including the President's daughter. Dont worry. They are safe in a secret location.
Send me 1 Billion CoCanDs 🤑 in cash 💸 with a spaceship 🚀 and my autonomous bots will safely bring back your citizens.

I heard that CoCanDians have the best brains in the Universe. Solve the puzzle I sent as an attachment for the next steps.

I'm approximately 12.8 light minutes away from the sun and my advice for the puzzle is

"Don't Trust Your Eyes"

Lol 😂

See you Major. Waiting for the Cassshhhh 💰

Continuing looking at the email, it showed another base64 encoded content which is supposed to be from a PDF file called "PuzzleToCoCanDa.pdf". Once again, I used CyberChef to decode the formatted content. Before I saved it, I changed the content into Hex format as shown below. The reason I did this is because I want to confirm if the file is really a PDF file. The first four bytes of a file makes up for what is called a file signature (or hex signature). In this case, the first four bytes of the hex signature are 50 4b 03 04.

```
--BOUND_600FB98E0DCEE8.49207210
Content-Type: application/pdf; name="PuzzleToCoCanDa.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="PuzzleToCoCanDa.pdf"
```

Output

< 1: Hi TheMajorOnEarth,The abducted CoCanDians are with ...

50 4b 03 04 14 00 00 00 08 00 20 85 39 52 08 0f c6 28

Using these four bytes, I visited the Gary Kessler Signature Files website (garykessler.net) to confirm if they correspond to a PDF file. As we can see below, PDF files have a hex signature of 25 50 44 46, which already tells me that the "PuzzleToCoCanDa.pdf" is not actually a PDF file.

25 50 44 46   %PDF
                          PDF, FDF, AI   Adobe Portable Document Format

Then, from CyberChef, I proceeded to save the decoded content from "PuzzleToCoCanDa.pdf" in a folder named *ATTACHMENT.ZIP*. Once I extracted it, it contained three items inside as shown in the image below.
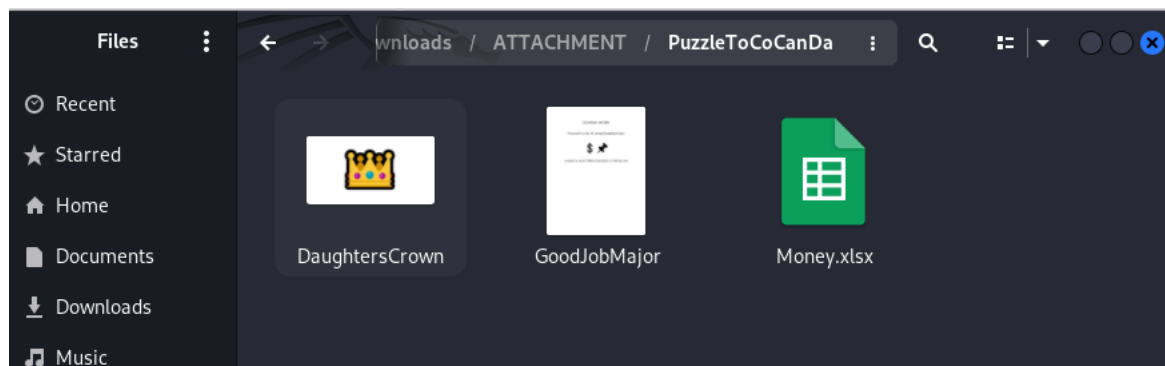
One of the items has an Excel file extension named "*Money.xlsx*". This time, before I confirm if it's an Excel file, I'm going to use HxD, a hex editor, to see the byte patterns of the file. After I opened the "*Money.xlsx.*" file in HxD, it gave me the hex signature of "50 4B 03 04" as shown below.
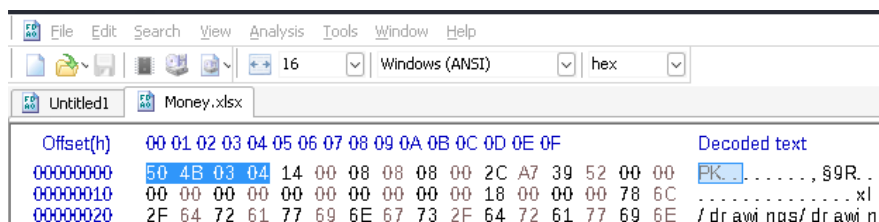
With this signature, I went back to Gary Kessler's website and confirmed that the signature identifies an Excel file extension.

Since my VM doesn't have an Excel program, I used another tool called Square X which has a file viewer where I can drag a file there and view it. After I dragged the "*Money.xlsx*" *file* into Square X, it showed the following message as shown in the image below:

	A	B
1		
2		
3		Whatever you have seen or read till now is fake. Our intension was not for money. It is the beginning of the WAR WITH CoCanDians
4		
5	Location	It's not that easy to find this Majorr!! I will also stay in the same location but I bet CoCanDian's cant do anything in my planet☻
6		
7		
8		Find and come ASAP I'm Waiting!
9		

The document had two sheet tabs. Sheet 1 had the above message, while the other tab (in this case it was called Sheet 3) had nothing in it as shown below.

Now, because this is a CTF (Capture the Flag) lab, a blank sheet wouldn't be put in here without a reason. One possible reason could be that a text is blended in using the color white. Therefore, I proceeded in clearing the format in both sheets to see if a hidden text appeared. Sheet 1 didn't reveal anything, but Sheet 3 revealed something as shown below:

	A	B	C	D	E	F	G	H
1								
2								
3								
4			VGhlIE1hcnRpYW4gQ29sb255LCBCZXNpZGUgSW50ZXJwbGFuZXRhcnkgU3BhY2Vwb3J0Lg==					
5								

Finally, I copied this text into CyberChef to decode it to reveal the message:

Input

VGhlIE1hcnRpYW4gQ29sb255LCBCZXNpZGUgSW50ZXJwbGFuZXRhcnkgU3BhY2Vwb3J0Lg==

ABC 72   ≡ 1

Output

The Martian Colony, Beside Interplanetary Spaceport.

Lastly, as part of the lab's objectives, I had to discover the name and last name of the malicious actor. To do that, I used *exiftool* to retrieve the metadata of the files inside the *ATTACHMENT.ZIP* folder. Of the three files, *GoodJobMajor*, revealed the author which is Pestero Negeja.

```
─$ exiftool GoodJobMajor
ExifTool Version Number         : 12.76
File Name                       : GoodJobMajor
Directory                       : .
File Size                       : 28 kB
File Modification Date/Time     : 2021:01:26 11:14:22-05:00
File Access Date/Time           : 2024:05:27 15:10:01-04:00
File Inode Change Date/Time     : 2024:05:27 15:07:35-04:00
File Permissions                : -rw-rw-r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.5
Linearized                      : No
Author                          : Pestero Negeja
Producer                        : Skia/PDF m90
Page Count                      : 1
```