

## Suspicious Email Analysis Field Guide

Brian T. Carr

Utica College

Center for Internet Security

### Author Note

Brian T. Carr is a Graduate Student at Utica College and an Intern at the Center for Internet Security on their Computer Emergency Response Team. Any correspondence should be directed to the Author's personal email address: [brian@briantcarr.com](mailto:brian@briantcarr.com).

### Abstract

“There are threats that (no matter how individualized one may feel) everyone still has to contend with. Phishing and general email security, Ransomware, and DoS are all potential issues that should be threat modeled and addressed. These topics may not seem new, but we still have not learned our lesson.” (Verizon, 2019, p. 40) The internet is a scary place, and it is often difficult to prioritize how to secure the computer systems connected to it. Currently, an exceedingly prominent attack vector is email; email messages may serve as a delivery mechanism for credential harvesting and credential-based attacks, as well as the delivery of malware. In the 2018 Internet Crime Report (ICR) published by the Internet Crime Complaint Center (IC3), it was reported that 26,379 victims experienced a Phishing/Vishing/Smishing/Pharming incident. These phishing incidents accounted for a total of \$48,241,748 in losses on behalf of those victimized. (Internet Crime Complaint Center, 2018) In the 2019 Verizon Data Breach Report, Verizon states that over 90% of detected malware was received through email. 78% of Cyber-Espionage incidents involved phishing. (Verizon, 2019) Phishing emails are heavily utilized by cybercriminals, and we must develop methods to systematically defeat them. Malicious threat actors only require a single phishing email to be successful, whereas cybersecurity professionals need to defend against all of them. The modern digital landscape requires end-users to use caution and vigilance. Analyzing phishing suspicious emails for malicious content is a service that the majority of users require.

*Keywords:* Phishing, Email, Social Engineering, Attack Vector, Analysis

## Table of Contents

Abstract .....	2
Suspicious Email Analysis Field Guide.....	5
Phishing .....	6
What is Phishing? .....	6
Suspicious Email Analysis Guide.....	8
Analysis Environment.....	8
Setting up an Email Address to Receive Suspicious Emails .....	9
Receiving Suspicious Emails in the Correct Format .....	10
Email Content Analysis.....	11
Email Header Analysis.....	21
Conclusion .....	26
Recommendations .....	27
Technical recommendations. ....	27
Organizational recommendations. ....	28
User recommendations.....	28
References .....	30
Appendix.....	32
Useful Email Analysis Tools .....	32

### Table of Figures

Figure 1: Snapshot tools shown within the VMware Workstation toolbar. ....	8
Figure 2: Connecting an Email Account to Mozilla Thunderbird. ....	10
Figure 3: Sample Suspicious Email. ....	11
Figure 4: VirusTotal Submission Page. ....	12
Figure 5: Sample VirusTotal Output. ....	13
Figure 6: Sample of Petya Infecting a Cisco ThreatGrid Sandbox VM. ....	14
Figure 7: ThreatGrid Sandbox Analysis Report. ....	14
Figure 8: Credential Harvesting Webpage. ....	15
Figure 9: Macro Warning for Sample Suspicious File. ....	16
Figure 10: Linux File Command Line Utility. ....	17
Figure 11: Exiftool Results for Sample Suspicious File. ....	18
Figure 12: Sample Suspicious Document Open Within the Bless Hexadecimal Editor. ....	19
Figure 13: Sample Suspicious File Header Within the File Header Table. (Kessler, 2019).....	19
Figure 14: Source Code of Sample Suspicious File Viewed with Vim. ....	20
Figure 15: Sample CyberChef Decryption. ....	21
Figure 16: Viewing an Emails Header in Thunderbird. ....	21
Figure 17: Email Header from Sample Suspicious Email. ....	22
Figure 18: First-Hop with an External IP Address. ....	24
Figure 19: Message-ID Field from Sample Suspicious Email Header. ....	24
Figure 20: Thumper Results for Sample Suspicious Email. ....	25
Figure 21: Message Header Analyzer Result for the Sample Suspicious Email. ....	26

### **Suspicious Email Analysis Field Guide**

Today, one would have to search for a while to locate a business that doesn't utilize email. Additionally, individuals have personal emails, businesses have business email, and nearly every entity has an email address associated with it. This seems great since now it is almost effortless to send a communication anywhere across the globe, but is there a downside? The more email addresses there are, the more targets there are for cybercriminals utilizing phishing email attack vectors. Unsuspecting individuals who carelessly click on hyperlinks, attachments, and emails that have the potential to be malicious leave systems vulnerable to exploitation. At the same time, it may not be realistic to expect every end-user to be able to vet their inbox for threats. Additionally, even the most experienced users are susceptible to social engineering attack vectors such as phishing emails. The Author believes that analyzing emails is a necessary function for every entity. Ideally, this function should be automated, but not every organization has an automated solution available to them. Currently, combining relevant security controls with manual analysis capabilities will significantly mitigate risk.

This guide is intended for individuals looking to analyze suspicious emails. This is not a guide on how to spot suspicious emails within one's inbox, nor is it a guide on responding to incidents attributed to phishing email attack vectors. This guide will not cover common mistakes in phishing emails, as to account for the more advanced phishing email attack vectors. Previously poor English and suspicious email addresses were clear-cut indicators of a phishing email. But, what about the phishing email authors who use proper grammar and choose to utilize email addressing schemes which promote legitimacy? By utilizing the techniques described within this guide, one should be able to reveal additional information regarding a phishing email. The Author hopes that his guide will help protect users from phishing email incidents. The degree to

which an email is analyzed is directly impacted by the resources available and the amount of time that can be allocated.

## **Phishing**

### **What is Phishing?**

The National Institute of Standard and Technology (NIST) defines phishing as, “Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.” (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016) Phishing email attack vectors are only a subgenre of phishing attack vectors. Phishing can be done through emails, text messages, phone calls, social media, and virtually any means of communication.

Phishing email attack vectors primarily have two functions: to distribute malware, and to harvest credentials or other information. Phishing emails attack vectors are used to distribute a variety of malware. CISA reports that phishing emails are a standard ransomware distribution method. (CISA, 2019) Cybercriminals utilize phishing emails with social engineering properties to entice users into infecting their system with malware or providing the attacker with their credentials. Additionally, it is possible that the phishing email attack vector is only the initial compromise vector in a larger campaign. The majority of the reported Advanced Persistent Threat (APT) intrusions including Operation Aurora, the HBGary Federal hack, and the RSA hack all began with phishing email attack vectors. (Yip, 2019) A more critical approach to assessing emails is necessary to mitigate risk associated with this type of threat. In many cases, the only way to truly determine if a suspicious email is a malicious email is to perform a manual email analysis.

**Why are phishing emails so successful?**

Malicious attackers may find that they have a higher rate of success when leveraging Phishing email attack vectors. This can be partially attributed to phishing emails implementing social engineering attributes along with technical attributes. “criminals successfully evade an organization’s security controls by using clever phishing and social engineering tactics that often rely on employee naivete.” (KnowBe4, 2019, p. 2) Social engineering attack vectors aim to convince the user to perform an unintentionally malicious action, which successfully subverts a majority of the technical controls commonly implemented. Usually, phishing emails attack vectors request users to perform common actions submit their credentials, download an attachment, or provide information.

**Common phishing attack vectors.**

Phishing— Communications with the intent of having the recipient disclose sensitive personal information through a malicious method.

Spear-Phishing— Communications targeted at a single entity with the intent of having the recipient disclose sensitive personal information through a malicious method.

Whaling— Communications targeted at senior executive or higher profile entities with the intent of having the recipient disclose sensitive personal information through a malicious method

Smishing— SMS (Text Message) communications with the intent of having the recipient disclose sensitive personal information through a malicious method.

Vishing— Communications sent via Voice over Internet Protocol (VoIP) with the intent of having the recipient disclose sensitive personal information through a malicious method.

### Suspicious Email Analysis Guide

#### Analysis Environment

When analyzing suspicious emails, one will commonly encounter some of the most malicious malware variants. This means that this type of analysis should only be completed on hardened systems. It helps to analyze the suspicious emails within a Linux virtual machine (VM), running on a host operating system. This will help to prevent malware from infecting the host machine. Although, it is important to remember that there are variants of malware with VM escaping characteristics. Keeping the VM, the host machine, and the hypervisor up to date will assist in mitigating the risk associated with VM escaping malware variants. (University of Hawaii, n.d.) Additional hardening and isolation features will help prevent incidental infections during analysis. When working with virtual machines it helps to take a clean Snapshot, so that it is easy to roll back the system to an uninfected state. The Snapshot tools within the VMware toolbar can be seen outlined in green within *Figure 1*.



*Figure 1: Snapshot tools shown within the VMware Workstation toolbar.*

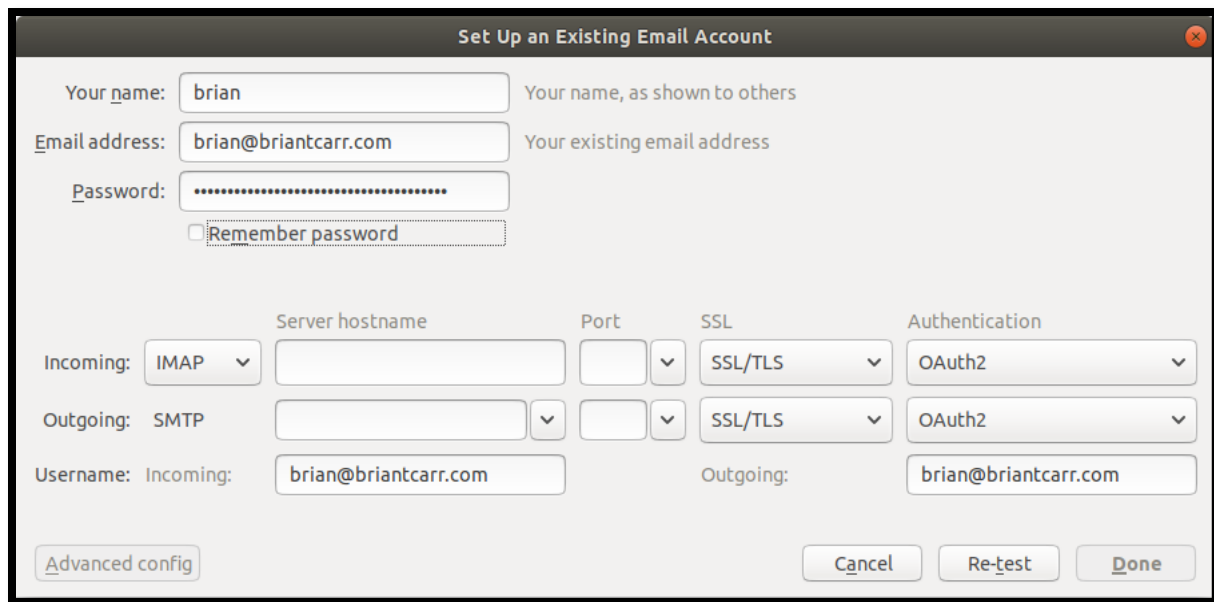
Typically, suspicious email analysis is not performed within an isolated malware lab as internet connectivity is often a necessity. Internet access is occasionally required when analyzing



suspicious emails. When internet access is necessary, additional technical controls will need to be implemented. It may be a good idea to configure your VM's network adapter as host only. This way whenever the internet is needed, it can be utilized after reconfiguring the VM's network adapter. There are a variety of Linux-based security tools that can help determine if the system has been compromised as the result of any unintended effects occurring as part of the analysis. These include Sophos Antivirus for Linux, Comodo Antivirus, ClamAV, Rootkit Hunter. It is recommended to implement one or more of these tools for monitoring, and in the event of an incident, it is best to roll back to the clean state, instead of attempting to quarantine the malware.

### **Setting up an Email Address to Receive Suspicious Emails**

This can be done with a variety of email solutions. If the intention is to implement the suspicious email inbox on an existing domain, the Author recommends creating a separate VLAN for the "dirty network". If the intention is to set this up quickly, a public email solution such as Gmail, Yahoo Mail, or Proton Mail will work sufficiently. Mozilla Thunderbird is an email application that functions well on the Linux platform. You can configure Thunderbird to send and receive emails from your email solution. The Thunderbird configuration screen which can be seen in *Figure 2*.

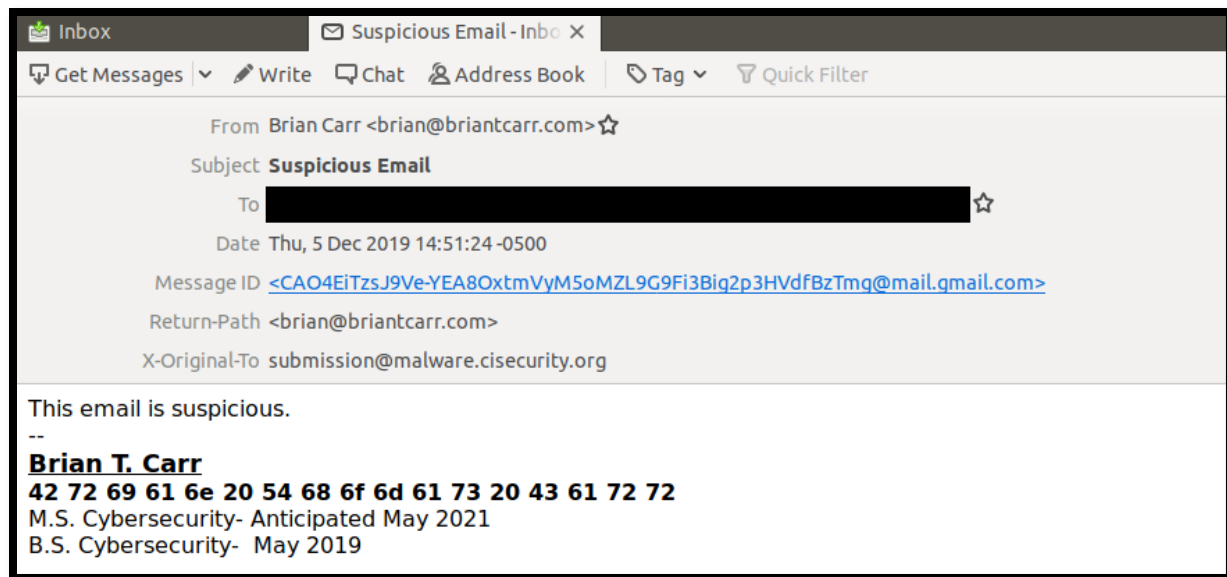


The screenshot shows the 'Set Up an Existing Email Account' dialog box in Mozilla Thunderbird. The dialog has a title bar with a close button. It contains several input fields and dropdown menus. The 'Your name' field is filled with 'brian'. The 'Email address' field is filled with 'brian@briantcarr.com'. The 'Password' field is filled with a series of dots. There is a checkbox for 'Remember password' which is unchecked. Below these fields are two rows of settings for 'Incoming' and 'Outgoing' mail. The 'Incoming' row has 'IMAP' selected for the protocol, an empty field for the server hostname, an empty field for the port, 'SSL/TLS' selected for SSL, and 'OAuth2' selected for authentication. The 'Outgoing' row has 'SMTP' selected for the protocol, an empty field for the server hostname, an empty field for the port, 'SSL/TLS' selected for SSL, and 'OAuth2' selected for authentication. At the bottom, there are two fields for 'Username': 'Incoming' is filled with 'brian@briantcarr.com' and 'Outgoing' is filled with 'brian@briantcarr.com'. At the very bottom are three buttons: 'Advanced config', 'Cancel', 'Re-test', and 'Done'.

Figure 2: Connecting an Email Account to Mozilla Thunderbird.

## Receiving Suspicious Emails in the Correct Format

Many email analysis tools require the email to be in a plaintext format. By saving an email or forwarding it as an attachment, one would see that the email becomes a file with an EML extension. This file contains the email header in a plaintext format. If an email is directly forwarded, then the email header has been overwritten. To ensure that the suspicious email is received in the right format, it may be worth explaining to all submitters that emails must be forwarded as attachments, as opposed to forwarding them traditionally. In addition to providing the email header in a plaintext format, EML files are also able to be opened by any email application. A sample suspicious email can be seen in *Figure 3*.



*Figure 3: Sample Suspicious Email.*

## Email Content Analysis

Once the malicious email is in the inbox, the easiest option may be to browse it for overtly malicious content. Typical malicious content includes hyperlinks, attachments, and tracking pixels. Hyperlinks and attachments may be easier to analyze through an email application as opposed to analyzing them within email headers. It is possible to extract a hyperlink or an attachment from an .eml file without opening the file, but it will likely be encoded. Hyperlinks and attachments can be both manually and automatically analyzed. Manual analysis may be time-consuming, and many of the artifacts found can also be found with automated analysis. For the automated portion of the email content analysis, hyperlinks and attachments should be processed by a sandbox solution prior to any further analysis. In the event that a sandbox is not available, VirusTotal may be the best solution for determining if an artifact is malicious. VirusTotal allows you to search by a variety of indicators including uploading the entire file, URL or hash values, to determine if there are any matches. Websites or files

previously marked as malicious will likely be flagged by VirusTotal. The VirusTotal submission page can be seen in *Figure 4*.



*Figure 4: VirusTotal Submission Page.*

To show what the output of VirusTotal looks like, an MD5 hash of a known malicious email attachment was submitted to VirusTotal. The MD5 hash was flagged as malicious by twenty-one antivirus solutions, this can be seen in *Figure 5*. The 'Details', 'Relations', 'Behavior' and 'Community' tabs contain additional information regarding the MD5 hash value submitted. If VirusTotal provides no malicious indicators, that does not mean that the file is innocuous. It is important to remember that just because the item in question was not flagged as malicious does not mean that it is safe. This is one shortcoming of using VirusTotal as opposed to an automated sandbox solution. Sandbox solutions will provide relevant Indicators of Compromise (IOC), which are extremely useful during the remediation process. In the event of

an incident, running the malicious artifact through an automated sandbox solution may be the easiest way to IOCs which can be located on any infected systems.

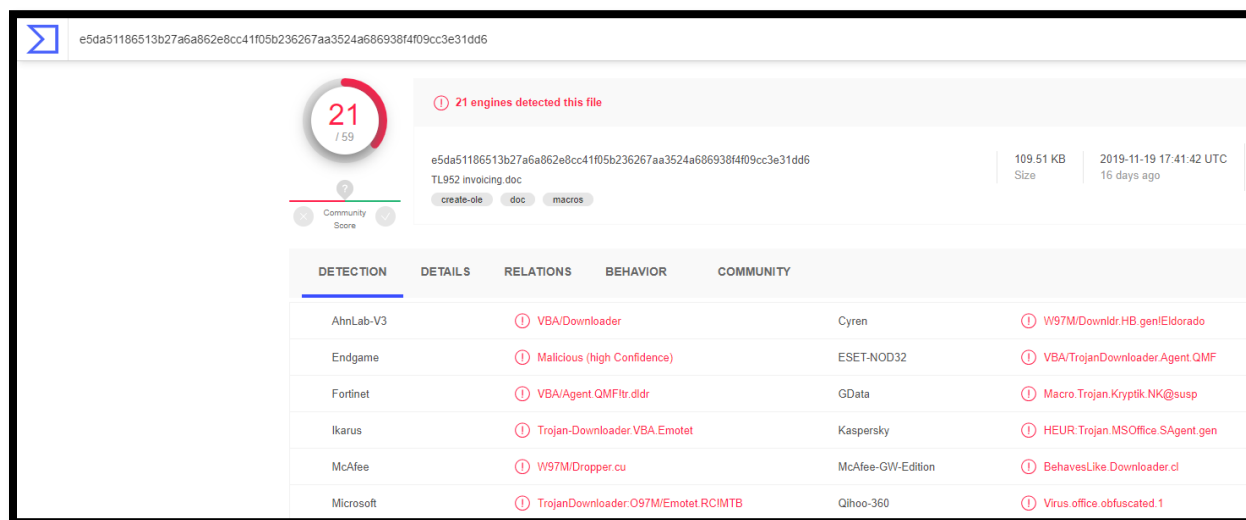


Figure 5: Sample VirusTotal Output.

Cisco maintains a powerful automated sandbox solution known as ThreatGrid. To show how an automated sandbox solution processes a malicious file, the Author submitted a copy of the Petya ransomware variant binary to Cisco ThreatGrid. A ThreatGrid sandbox virtual machine (VM) infected with Petya ransomware can be seen in *Figure 6*. Once the analysis is complete the sandbox will provide a comprehensive report which includes behavioral indicators, network streams, associated processes, artifacts, registry activity, and file activity. This information is extremely valuable to anyone attempting to recover from a malware incident. The Cisco ThreatGrid report for the NotPetya binary can be seen in *Figure 7*.

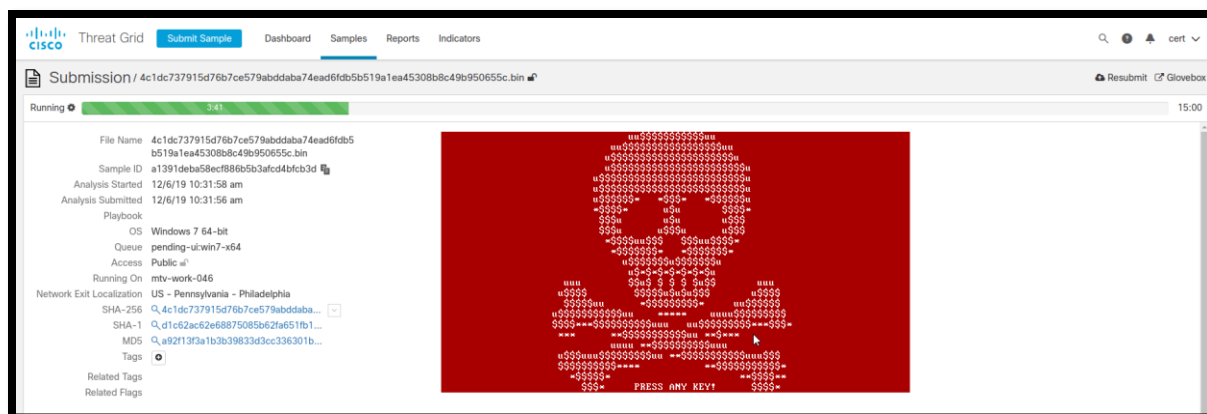


Figure 6: Sample of Petya Infecting a Cisco ThreatGrid Sandbox VM.

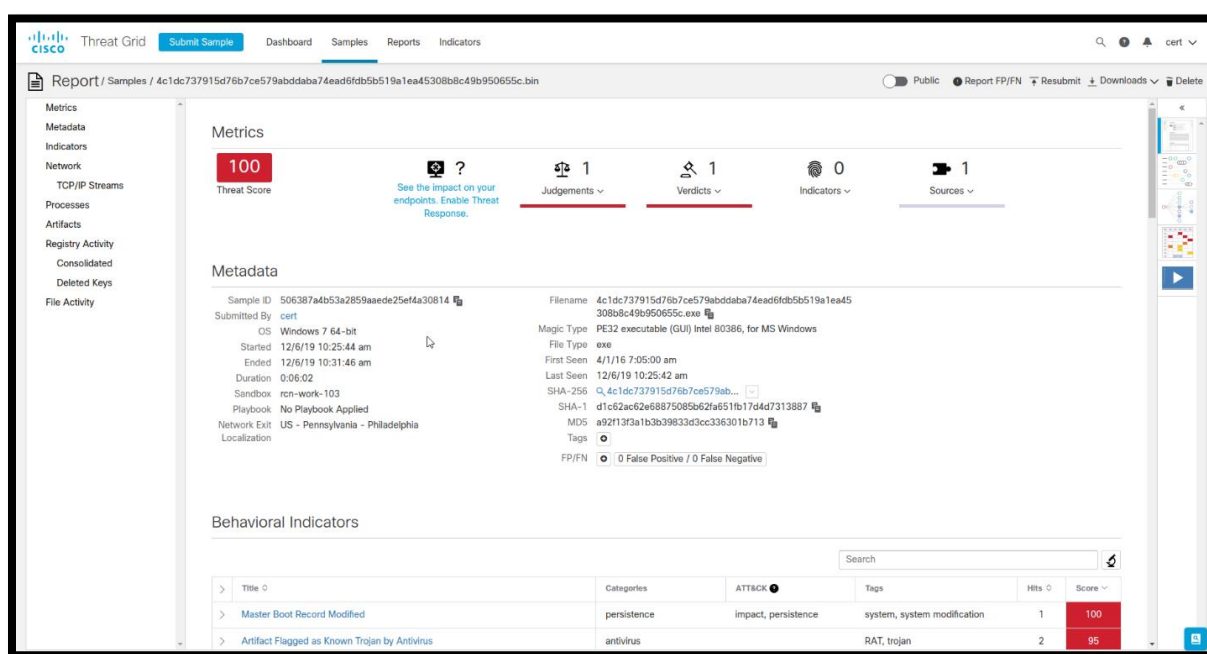
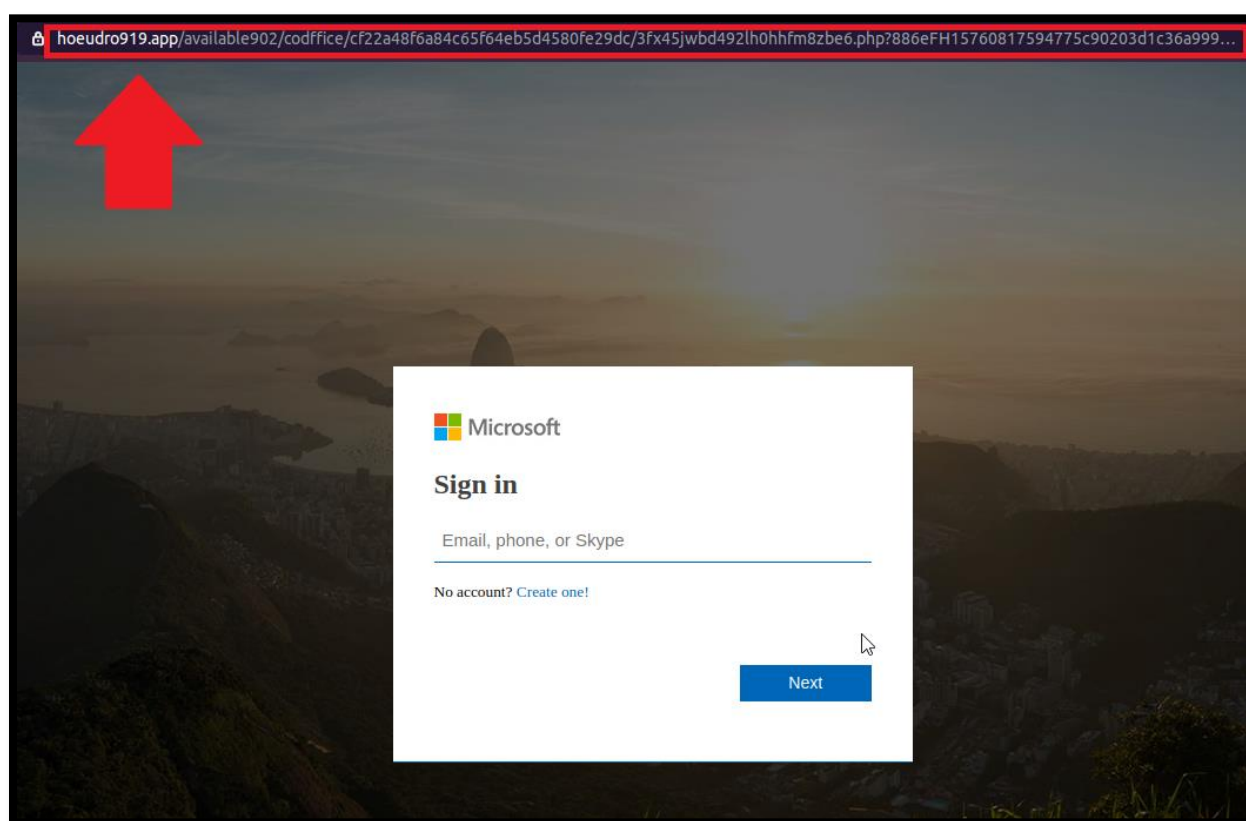


Figure 7: ThreatGrid Sandbox Analysis Report.

Manually analyzing hyperlinks should always be done using Tor within a virtual machine environment. Tor can be utilized through the Tor browser which is built upon Mozilla's Firefox browser, or through the Brave browser's Tor plugin. Tor is utilized to anonymize web traffic by utilizing Tor nodes within the Tor network. (Porup, 2019) This will help to protect the identity you and your network when you navigate to a suspicious hyperlink. Although, this will not protect your system from malware associated with the hyperlink. Suspicious hyperlinks may provide attackers with a variety of functionalities. Often hyperlinks will lead to credential

harvesting webpages. A credential harvesting webpage can be seen in *Figure 8*. Other hyperlinks may guide a user to download a potentially malicious file from a file-sharing site, contain browser-based exploits such as HTTP buffer overflows, links to watering hole attacks, and even more. Utilizing both automated and manual analysis techniques may provide additional IOCs.



*Figure 8: Credential Harvesting Webpage.*

When manually analyzing malicious files there are many different approaches one can take. It is important to keep in mind that many of the IOCs that can be obtained from malicious files can be obtained in a variety of ways, so there is no one correct way to analyze a suspicious file. The techniques described in this section may be useful, but this is not intended to be a comprehensive malware reverse engineering guide.

To highlight the techniques described in this section, the Author utilized a potentially malicious Word document named Suspicious.doc. In this case, the Author knows that the file is a

malicious word document. Since the Author knows that the file is a malicious Word document, the first step taken was to open the document in an application that can view Word documents other than Microsoft Word. In this instance, the Author utilized Libre Office Writer. This program is an open-source alternative to the Microsoft Word application. Upon opening the sample suspicious file in Libre Office Writer, the application presented a warning that the document contained macros. The macro warning can be viewed in *Figure 9*. Microsoft Office document macros, which typically include Visual Basic for Applications (VBA) scripts, are often abused for the purpose of malware distribution. (Microsoft, 2019) There are static analysis tools that can analyze malicious macros such as ViperMonkey, but they will not be covered within this guide.

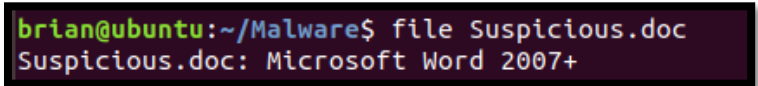


*Figure 9: Macro Warning for Sample Suspicious File.*

In the event that you do not know the file type, you may need to take some steps to locate that information. To determine the filetype of a suspicious file, the Linux command-line “File” utility can be utilized. The File command-line utility can be seen in *Figure 10*. A file’s metadata often contains valuable information including the file owner and important dates. Exiftool results for the sample suspicious file can be seen in *Figure 11*. If both Exiftool and the File utility claim



that the file has a filetype that does not match the extension, the file header can be further analyzed to determine the true filetype. To view the file header, the file will need to be opened within a hexadecimal editor. The file “Suspicious.doc” can be seen open within the Bless hexadecimal editor in *Figure 12*. The file header of Suspicious.doc was determined to have a file header of 50 4B 03 04 14 00 06. When compared with the resources located at [https://www.garykessler.net/library/file\\_sigs.html](https://www.garykessler.net/library/file_sigs.html), it was determined to be a Microsoft Office Open XML Format (OOXML) Document. The association between the filetype and file header can be seen in *Figure 13*. In this case, the file type revealed through Exiftool was verified through a file header analysis.



```
brian@ubuntu:~/Malware$ file Suspicious.doc
Suspicious.doc: Microsoft Word 2007+
```

*Figure 10: Linux File Command Line Utility.*

```
brian@ubuntu:~/Malware$ exiftool Suspicious.doc
ExifTool Version Number      : 10.80
File Name                    : Suspicious.doc
Directory                    : .
File Size                    : 61 kB
File Modification Date/Time   : 2019:12:02 12:57:58-05:00
File Access Date/Time        : 2019:12:12 11:47:14-05:00
File Inode Change Date/Time   : 2019:12:12 11:46:52-05:00
File Permissions              : rw-r--r--
File Type                    : DOCM
File Type Extension          : docm
MIME Type                    : application/vnd.ms-word.document.macroEnabled
Zip Required Version          : 20
Zip Bit Flag                  : 0x0006
Zip Compression              : Deflated
Zip Modify Date               : 1980:01:01 00:00:00
Zip CRC                      : 0xc8e48bf2
Zip Compressed Size          : 426
Zip Uncompressed Size        : 1635
Zip File Name                 : [Content_Types].xml
Template                     : Normal.dotm
Total Edit Time               : 0
Pages                        : 1
Words                        : 0
Characters                   : 0
Application                  : Microsoft Office Word
Doc Security                  : None
Lines                        : 2
Paragraphs                   : 0
Scale Crop                   : No
Heading Pairs                 : Название, 1, Title, 1
Titles Of Parts               : ,
Manager                      :
Company                      : home
Links Up To Date              : No
Characters With Spaces        : 0
Shared Doc                   : No
Hyperlinks Changed           : No
App Version                   : 16.0000
Title                        :
Subject                      :
Creator                      : tdcxqwi
Keywords                     :
Description                   :
Last Modified By              : admin
Revision Number               : 2
Create Date                   : 2019:12:02 09:31:00Z
Modify Date                   : 2019:12:02 09:31:00Z
Category                     :
brian@ubuntu:~/Malware$
```

Figure 11: Exiftool Results for Sample Suspicious File.

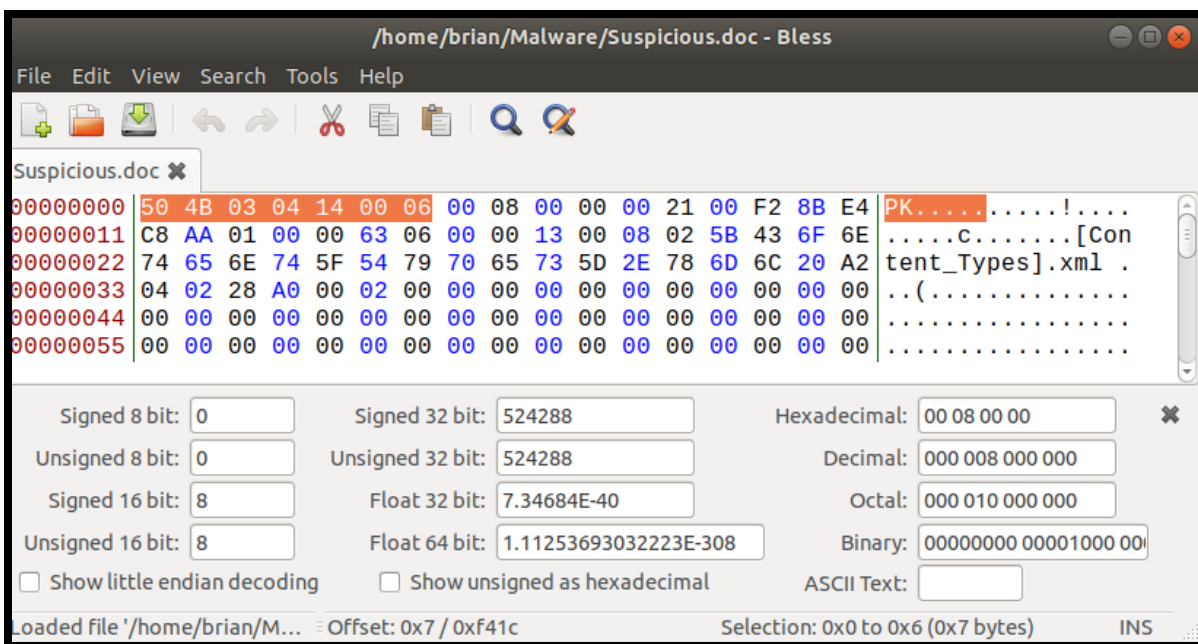


Figure 12: Sample Suspicious Document Open Within the Bless Hexadecimal Editor.

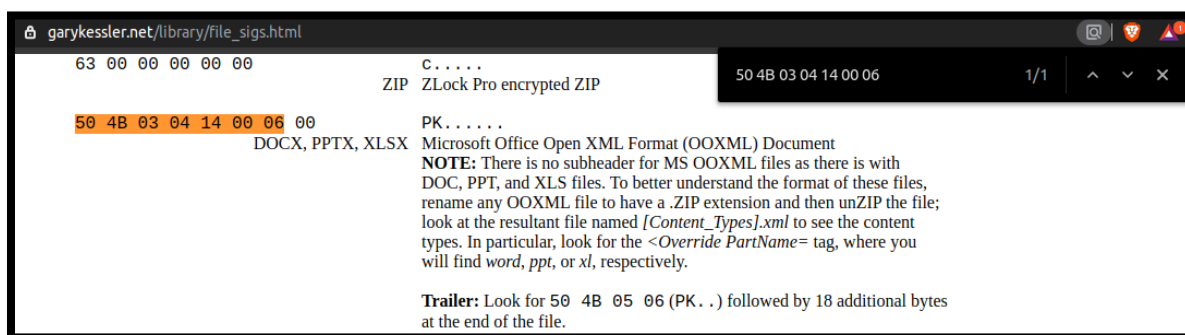


Figure 13: Sample Suspicious File Header Within the File Header Table. (Kessler, 2019)

Next, the sample suspicious file was opened within the Vim text editor. Suspicious.doc can be seen open within Vim in Figure 14. It can be seen in Figure 14 that the source code is not in a human-readable format, and will need to be parsed to provide more information.

Figure 14: Source Code of Sample Suspicious File Viewed with Vim.

There are plenty of freely available resources on the internet which provide a deeper dive into code analysis. This field guide only brushed upon a few on the quickest and easiest techniques that can be applied during analysis.

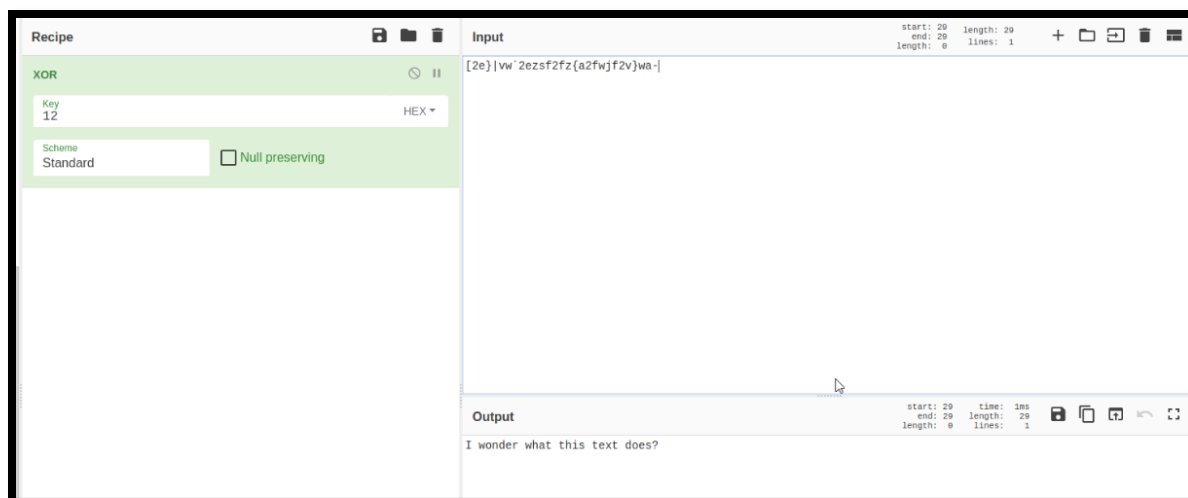


Figure 15: Sample CyberChef Decryption.

## Email Header Analysis

Analyzing the email header should reveal much of the same information located within the content analysis. An email header will contain information regarding where the email came from, the route it took, and much more. Anything located within the body of the email during the content analysis should also show up during the email header analysis. Although, you will generally find that it is Base64-encoded. The email header can be viewed by either opening the .eml file in a text editor or by opening the suspicious email in Mozilla Thunderbird and selecting 'View Source' from the 'More' menu with the Mozilla Thunderbird application. The 'View Source' button within Mozilla Thunderbird can be seen in *Figure 16*.

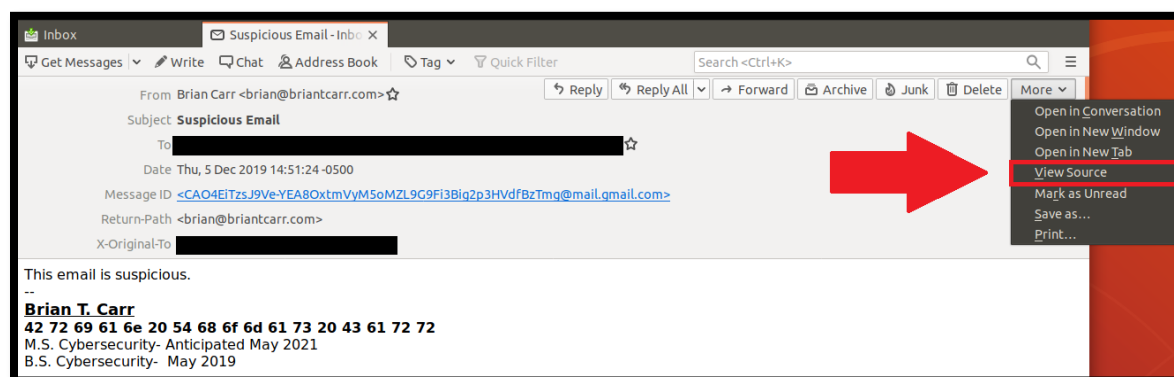


Figure 16: Viewing an Emails Header in Thunderbird.

The opened email header can be viewed in *Figure 17*. Email headers often look very different than one another. It is possible to analyze a suspicious email without the assistance of any additional tools, but the tools help to provide context and speed up the process. In some emails, the header may be hundreds if not thousands of lines. Some specific artifacts that typically provide additional information.

```
Return-Path: <brian@briantcarr.com>
X-Original-To: [REDACTED]
Delivered-To: [REDACTED]
Received: from mail-pg1-f180.google.com (mail-pg1-f180.google.com [209.85.215.180])
  by [REDACTED] (Postfix) with ESMTP id 0760AB8894
  for [REDACTED]; Thu, 5 Dec 2019 19:51:36 +0000 (UTC)
Received: by mail-pg1-f180.google.com with SMTP id k3so1433378pgc.3
  for [REDACTED]; Thu, 05 Dec 2019 11:51:35 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=briantcarr-com.20150623.gappssmtp.com; s=20150623;
  h=mime-version:from:date:message-id:subject:to;
  bh=rtbtm5s9HjpnprpXRYkPb5cKDjFGGp9YHU1xuQxU1W4=;
  b=bw7Cj9z7cEPEAgxyxJTIKjp5kpl0y30db27+0rIeINrJgnQnX02Y+aQ5L/RtErS7G
  v0+5t1Jncnw2Knp20isrop0wmZgT5jDj0YCIy2Gap2i5g3FRJqT93V1Uzq8B0Gk0U02t
  MxQkzwq8oeJWQ4KV+FgBZX6RwMorGAPdFMABupDFQH32G4hbAwtGtASWh0rEBG1yz5c1
  ms/V7UW9M+9XMqxYZ3I1+4soy8a6f2lhkdmXdyN0LAXELwcNLYSMHJ2qhFRjo5RSTfzi
  Y7+oAYmudwbxExeS6MQ5WeVRFLEunbL0ZvUHOz78Fs18Yu8/5ca0AX8Kq3FFaP0X6Swo
  p9UA==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=1e100.net; s=20161025;
  h=x-gm-message-state:mime-version:from:date:message-id:subject:to;
  bh=rtbtm5s9HjpnprpXRYkPb5cKDjFGGp9YHU1xuQxU1W4=;
  b=TQbrM/SBYFSbKZ4fiePoiFaQECb45Ze1Pn8njbw8XA44kIe4CREif7cZk2F3jUzFx
  RfGrb+rAKPZw3CXmbQ7fq6xo8F18elQcNtAVko383eUsGztoh7fLJbuy8LcT3RrdbCq
  ucp3NMfVgHVRV61ZSiXBneLT8pq+evnCNXLPV4Qk988Jtr8S8Q58KdSSzS5FMsXLQ+c
  oWtMe+rFo0ZtoQFswgplGwNeA0bAI404WPFOeYCJZtKRjDlhFVMWYLpeqiBTbC5LfJe
  bkSh9EVS4cYvYyouICNHldV42yENU8T/40W+n5cZZTeeD7onPJ08RbhrTtj2wqBgLP
  EFHQ==
X-Gm-Message-State: APjAAAXDqshM/TZpcVh0hpfFsxaiduopt2UebJS1Z6SuyheimPstULYp
  SfUTgNjZ4Mc40fqGmIt/GmyUEuWN5wi9a0lgjxywJL0hF4=
X-Google-Smtp-Source: APXvYqxc0ZvzPBK+aaDVVSZM/1Tk/Ggx9pgbilgYp/9htDxg2syHUhPtl7DsvyPULR9GEo8UV0d89XXdjrfAm10/hY=
X-Received: by 2002:aa7:9189:: with SMTP id x9mr10802412pfa.41.1575575495124;
  Thu, 05 Dec 2019 11:51:35 -0800 (PST)
MIME-Version: 1.0
From: Brian Carr <brian@briantcarr.com>
Date: Thu, 5 Dec 2019 14:51:24 -0500
Message-ID: <CA04Ei7zSJ9Ve-YEA80xtmVyM5oMZL9G9Fi38ig2p3HVdfBzTmg@mail.gmail.com>
Subject: Suspicious Email
To: [REDACTED]
Content-Type: multipart/alternative; boundary="00000000000b43c150598fa41a8"

--00000000000b43c150598fa41a8
Content-Type: text/plain; charset="UTF-8"

This email is suspicious.
--
*Brian T. Carr*
*42 72 69 61 6e 20 54 68 6f 6d 61 73 20 43 61 72 72*
M.S. Cybersecurity- Anticipated May 2021
B.S. Cybersecurity- May 2019

--00000000000b43c150598fa41a8
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable

<div dir=3D"auto">This email is suspicious.</div>--<br><div dir=3D"ltr" cl=
ass=3D"gmail_signature" data-smartmail=3D"gmail_signature"><div dir=3D"ltr">
<div dir=3D"ltr"><font size=3D"4"><u><b>Brian T. Carr</b></u></font><=
/div><div dir=3D"ltr"><b>42 72 69 61 6e 20 54 68 6f 6d 61 73 20 43 61 72 72=
</b><br></div><div dir=3D"ltr">M.S. Cybersecurity- Anticipated May 2021<br>=
<div>B.S. Cybersecurity- C2=A0 May 2019</div><div><br></div></div></d=
iv></div>

--00000000000b43c150598fa41a8--
```

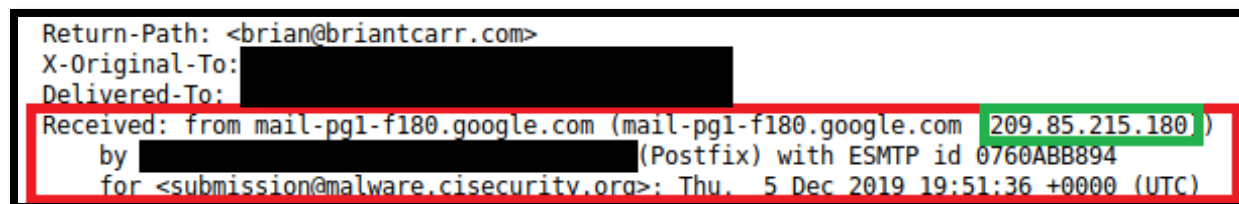
Figure 17: Email Header from Sample Suspicious Email.

There are a variety of fields within the email header, and many email solutions add additional header fields. On top of that, the email header information is subject to manipulation by anyone technically inclined enough to do so. To determine where the email traces back to, the hops within the email header should be analyzed. A hop refers to the email being sent between servers before reaching its destination. Each individual email hop is written with the sending address first, and the receiving address second. It can be thought about as the first Internet Protocol (IP) address in the last line starting with 'Received:'. Another way to think about this is that the email headers are written with the most recent hop at the top of the email header, and the least recent would be furthest down hop in the email header. The least recent hop would be the first-hop. In the event that the address is a private IP address, you should locate the first external IP address in the hops. The first-hop coming from an external IP address from within the sample suspicious email can be seen in *Figure 18*. There are various header fields with can assist in determining the authenticity of an email. Sender Policy Framework (SPF) is an email security protocol that is intended to prevent spam by detecting indicators of email spoofing. (Carranza, 2015) An SPF fail would indicate that the email is being sent from an IP address that does not match the addresses specified in the list of legitimate servers defined in any SPF policy applied to the sending domain. It may be difficult to locate the originating IP address from an email header just by reading it. In the case of the sample suspicious email, the email traces back to 209.85.215[.]180.

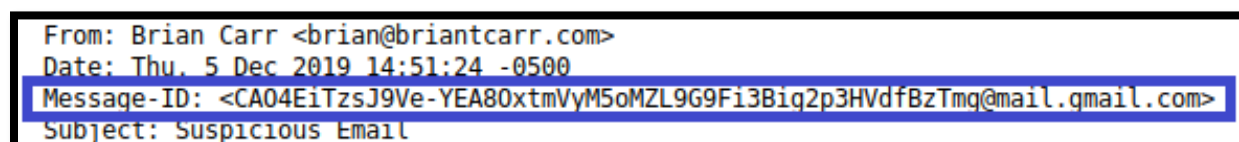
To determine the domain in that an email was sent from, the Message-ID field can be analyzed. The Message-ID property for the sample suspicious email can be found highlighted in blue within *Figure 19*. The sample suspicious email has a Message-ID that identifies it as coming from a server on the mail.gmail.com subdomain. This information can be compared with the IP



address the email traces back to in order to locate evidence of spoofing. Other fields of interest that were not contained within the sample suspicious email include, X-Originating-IP, Originating-Client, Envelope-ID, and User-Agent. It is important to keep in mind that there are numerous other fields. A list of all the email header fields can be located at <https://www.iana.org/assignments/message-headers/message-headers.xhtml>.

A screenshot of an email header section. The text is as follows: Return-Path: <brian@briantcarr.com>, X-Original-To: [REDACTED], Delivered-To: [REDACTED], Received: from mail-pg1-f180.google.com (mail-pg1-f180.google.com 209.85.215.180) by [REDACTED] (Postfix) with ESMTP id 0760ABB894 for <submission@malware.cisecurityv.org>; Thu, 5 Dec 2019 19:51:36 +0000 (UTC). The 'Received' line is highlighted with a red rectangular box, and the IP address '209.85.215.180' is highlighted with a green rectangular box.

*Figure 18: First-Hop with an External IP Address.*

A screenshot of an email header section. The text is as follows: From: Brian Carr <brian@briantcarr.com>, Date: Thu, 5 Dec 2019 14:51:24 -0500, Message-ID: <CA04EiTzsJ9Ve-YEA80xtmVyM5oMZL9G9Fi3Biq2p3HVdfBzTmq@mail.gmail.com>, Subject: Suspicious Email. The 'Message-ID' line is highlighted with a blue rectangular box.

*Figure 19: Message-ID Field from Sample Suspicious Email Header.*

To put these fields into a more readable format, it may prove valuable to use an email header analysis tool. The Author wrote a bash parser known as Thumper which outputs parsed information from a .eml file. The Thumper results for the sample suspicious email can be seen in *Figure 20*. The output of Thumper shows relevant information including the first-hop, all hops, located IP addresses, located email addresses, SPF information, client information, and Message-ID. The sample suspicious email did not contain each of the fields Thumper searches for. Each line of plus signs indicates that a search performed by Thumper yielded no results. Some important things to note are that the first-hop address was actually from an internal IPv6 address. This means that the first external IP address should be located within the email hops. Thumper is not the most comprehensive and beautiful email header analyzer.



The GitHub user lnxg33k released a python program named Message Header Analyzer, which provides the user with a graphical application local to their system which can parse information from an email header. The Message Header Analyzer results for the sample suspicious email can be found in *Figure 21*.

```

brian@ubuntu:~/Desktop/Suspicious_Email$ ./thumper.sh
Enter File name...: suspicious_email.eml

Information regarding first hop:
32-X-Received: by 2002:aa7:9189:: with SMTP id x9mr10802412pfa.41.1575575495124;
33- Thu, 05 Dec 2019 11:51:35 -0800 (PST)
34-MIME-Version: 1.0
35-From: Brian Carr <brian@briantcarr.com>

All hop information:
1-Return-Path: <brian@briantcarr.com>
2-X-Original-To: submission@malware.cisecurity.org
3-Delivered-To: submission@malware.cisecurity.org
4-Received: from mail-pg1-f180.google.com (mail-pg1-f180.google.com [209.85.215.180])
5-   by [REDACTED] (Postfix) with ESMTTP id 0760ABB894
6-   for [REDACTED] Thu, 5 Dec 2019 19:51:36 +0000 (UTC)
7-Received: by mail-pg1-f180.google.com with SMTP id k3so1433378pgc.3
8-   for [REDACTED] Thu, 05 Dec 2019 11:51:35 -0800 (PST)
9-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
10-   d=briantcarr-com.20150623.gappssmtp.com; s=20150623;
11-
12-
29-X-Gm-Message-State: APjAAAXDqshM/TZpcVh0hppFsxaaiduopt2UebJS1Z6SuyheimPstULYp
30-   SfuTgNjZ4Mc40fqGmIt/GmyUEuWN5wi9a0lgjxywJL0hF4=
31-X-Google-Smtp-Source: APXvYqxc0ZvzPBK+aaDVVSZM/1Tk/Ggx9pgbilgYp/9htDxg2syHUhPtL7DsvyPULR9GEo8UV0d89XXdjrfcAn10/hY=
32-X-Received: by 2002:aa7:9189:: with SMTP id x9mr10802412pfa.41.1575575495124;
33- Thu, 05 Dec 2019 11:51:35 -0800 (PST)
34-MIME-Version: 1.0
35-From: Brian Carr <brian@briantcarr.com>

The IPv4 addresses located in context:
4-Received: from mail-pg1-f180.google.com (mail-pg1-f180.google.com [209.85.215.180])

Here is a list of the IPv4 addresses and how many times they were located:
1 209.85.215.180

The IPv6 addresses in context:
32-X-Received: by [REDACTED] with SMTP id x9mr10802412pfa.41.1575575495124;

A list of IPv6 addresses and how many times they were located:
1 [REDACTED]

Here is a list of Email addresses and how many times they occurred:
2 brian@briantcarr.com
1 CA04EiTsJ9Ve-YEA80xtmVvM5oMZL9G9Fi3Big2p3HVdfBzTmg@mail.gmail.com
6 [REDACTED]

+++++
+++++
+++++
The Message-ID:
11:   h=mime-version:from:date:message-id:subject:to;
12:   bh=rtbtm5s9HjmpnrpXRYkPb5cKDjFGGp9YHU1xuQxU1W4=;
13:
21:   h=x-gm-message-state:mime-version:from:date:message-id:subject:to;
22:   bh=rtbtm5s9HjmpnrpXRYkPb5cKDjFGGp9YHU1xuQxU1W4=;
23:
37-Message-ID: <CA04EiTsJ9Ve-YEA80xtmVvM5oMZL9G9Fi3Big2p3HVdfBzTmg@mail.gmail.com>
38-Subject: Suspicious Email
=====
brian@ubuntu:~/Desktop/Suspicious_Email$

```

Figure 20: Thumper Results for Sample Suspicious Email.

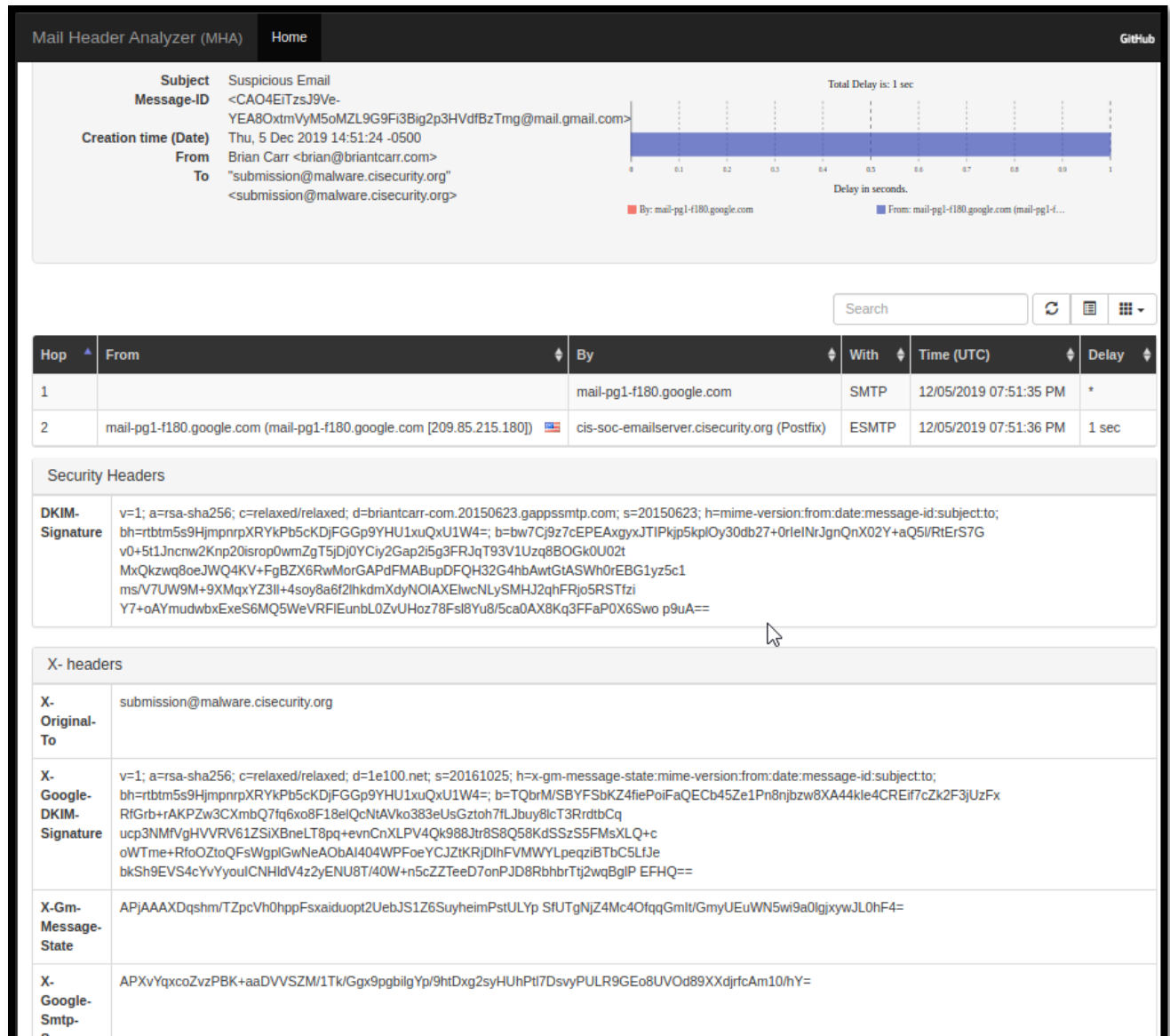


Figure 21: Message Header Analyzer Result for the Sample Suspicious Email.

## Conclusion

Suspicious emails flood the inboxes of users everywhere, and learning how to analyze these suspicious emails can help prevent incidents from occurring. There are various technical, organizational, and user awareness recommendations that assist in the mitigation of phishing email attack vectors. These recommendations can be found in the Appendix. Email has been determined to be a weak point in organizational security. Subsequently, entities need to

acknowledge this weak point as well as implement security controls to assist in risk mitigation. According to the 2018 ICR, phishing attack vectors caused 26,379 victims to lose a combined total of \$48,241,748. (Internet Crime Complaint Center, 2018, pp. 19-20) Researchers at Verizon explain that phishing email attack vectors are the most common point of entry for malware, “When the method of malware installation was known, email was the most common point of entry.” (Verizon, 2019, p. 13) Unfortunately, securing users from social engineering attack vectors cannot be done through technical controls alone. Awareness, experience, and familiarity will help users to develop a more critical perspective. But that being said, even the most experienced user can fall victim to a well-crafted phishing email attack vector. Performing email analysis may be the only way to determine if an email is truly malicious.

## **Recommendations**

The following recommendations were provided by the Multi-State - Information Sharing and Analysis Center located at the Center for Internet Security. In addition to implementing these recommendations, implementing the CIS Controls will provide organizations with an increased level of security. The Center for Internet Security explains the CIS controls as, “A prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.” (Center for Internet Security, 2019, p. 1)

### **Technical recommendations.**

- Flag emails from external sources with a warning banner.
- Implement filters at the email gateway to sift out emails with known phishing indicators, such as known malicious subject lines, and block suspicious links.
- Adhere to the Principle of Least Privilege. If a user has no need for administrative access in order to carry out their daily activities, they should not have an

administrative account. This can minimize the damage caused by malicious activity carried out under the user's credentials.

- Implement Domain-based Message Authentication, Reporting, & Conformance (DMARC), a validation system that minimizes spam emails by detecting email spoofing using Domain Name System (DNS) records and digital signatures.
- Implement Sender Policy Framework (SPF), an email authentication method used to detect spoofed sender addresses.

#### **Organizational recommendations.**

- Provide social engineering and phishing training to employees. Urge them not to open suspicious emails, click links contained in such emails, post sensitive information online, and never provide usernames, passwords, and/or personal information to any unsolicited request.
- Conduct organized phishing exercises to test and reinforce the concepts using services such as those provided by CIS.
- Implement a standardized protocol for reporting phishing attempts to the Information Technology (IT) department.

#### **User recommendations.**

- Do not open suspicious emails or click on unknown links. The easiest way to check a link is by hovering over it with your mouse. This allows the true destination of the link to appear in the bottom left corner of your browser window or next to your mouse pointer in Microsoft Outlook.
- Never reveal personal or financial information in response to an email. Legitimate organizations will never ask for this information in an unsolicited email.

If the message appears to be a phishing email, do not respond. Report it to the IT department immediately and await further instruction.

(MS-ISAC, 2018)

## References

- Carranza, P. (2015, April 20). *How To use an SPF Record to Prevent Spoofing & Improve E-mail Reliability*. Retrieved from digitalocean.com:  
<https://www.digitalocean.com/community/tutorials/how-to-use-an-spf-record-to-prevent-spoofing-improve-e-mail-reliability>
- Center for Internet Security. (2019, April 1). *CIS Controls*. Retrieved from cisecurity.org:  
<https://www.cisecurity.org/controls/>
- CISA. (2019, December 11). *Ransomware*. Retrieved from us-cert.gov: <https://www.us-cert.gov/Ransomware>
- Internet Crime Complaint Center. (2018). *2018 Internet Crime Report*. Retrieved from ic3.gov:  
[https://pdf.ic3.gov/2018\\_IC3Report.pdf](https://pdf.ic3.gov/2018_IC3Report.pdf)
- Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016, October). *NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing*. Retrieved from nist.gov: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>
- Kessler, G. (2019, December 17). *GCK'S FILE SIGNATURES TABLE*. Retrieved from garykessler.net: [https://www.garykessler.net/library/file\\_sigs.html](https://www.garykessler.net/library/file_sigs.html)
- KnowBe4. (2019). *Phishing by Industry Benchmark Report 2019*. KnowBe4.
- Microsoft. (2019, August 13). *Getting started with VBA in Office*. Retrieved from microsoft.com:  
<https://docs.microsoft.com/en-us/office/vba/library-reference/concepts/getting-started-with-vba-in-office>
- Microsoft. (2019, September 04). *Macro malware*. Retrieved from microsoft.com:  
<https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/macro-malware>

- MS-ISAC. (2018, July). *MS-ISAC Security Primer Spear Phishing*. Retrieved from cisecurity.org: <https://www.cisecurity.org/wp-content/uploads/2018/07/MS-ISAC-Security-Primer-Spear-Phishing.pdf>
- Porup, J. (2019, October 15). *What is the Tor Browser? How it works and how it can help you protect your identity online*. Retrieved from <https://www.csoononline.com/>: <https://www.csoononline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html>
- University of Hawaii. (n.d.). *Building a Vulnerability/Malware Test Lab*. Retrieved from <https://westoahu.hawaii.edu/>: <https://westoahu.hawaii.edu/cyber/building-a-vulnerability-malware-test-lab/>
- Verizon. (2019, May 21). *2019 Data Breach Investigations Report*. Retrieved from [verizon.com: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf](https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf)
- Yip, K. N. (2019). *Phishing APTs (Advanced Persistent Threats)*. Retrieved from [infosecinstitute.com](https://resources.infosecinstitute.com/): <https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-as-an-attack-vector/phishing-apt-advanced-persistent-threats/>

## Appendix

### Useful Email Analysis Tools

Tool Name	URL	Description
Thumper	<a href="https://www.github.com/carrcybersec/thumper">https://www.github.com/carrcybersec/thumper</a>	Bash script that parses out email header information.
KnowBe4 Free Tools	<a href="https://www.knowbe4.com/resources">https://www.knowbe4.com/resources</a>	Variety of free IT security tools. Many of which specifically target email security.
Message Header Analyzer	<a href="https://github.com/lnxg33k/email-header-analyzer">https://github.com/lnxg33k/email-header-analyzer</a>	Graphical email header analyzer, written in Python.
MXToolBox Email Header Analyzer	<a href="https://mxtoolbox.com/EmailHeaders.aspx">https://mxtoolbox.com/EmailHeaders.aspx</a>	Web application that helps to parse information from email headers.
G Suite ToolBox MessageHeader	<a href="https://toolbox.googleapps.com/apps/messageheader/">https://toolbox.googleapps.com/apps/messageheader/</a>	Web application that helps to parse information from email headers.
VirusTotal	<a href="https://www.virustotal.com/gui/home/upload">https://www.virustotal.com/gui/home/upload</a>	Analyzes items and shares the indicators.
IPLocation	<a href="https://www.iplocation.net/">https://www.iplocation.net/</a>	Web application used to perform geo-location lookup on IP address and domain names.
CentralOps	<a href="https://centralops.net/co/">https://centralops.net/co/</a>	Variety of tools used for analyzing domains.
GoDaddy WHOIS	<a href="https://www.godaddy.com/whois">https://www.godaddy.com/whois</a>	WHOIS lookup tool provided by GoDaddy.
Shodan	<a href="https://Shodan.io">https://Shodan.io</a>	Search engine that can locate internet connected devices.
host.io	<a href="https://host.io/">https://host.io/</a>	Useful for domain data.
Whois.net	<a href="https://www.whois.net/">https://www.whois.net/</a>	Whois lookup tool.
ICANN Lookup	<a href="https://lookup.icann.org/">https://lookup.icann.org/</a>	Domain lookup tool.
CyberChef	<a href="https://gchq.github.io/CyberChef/">https://gchq.github.io/CyberChef/</a>	Static code analysis tool.



ViperMonkey	<a href="https://github.com/decalage2/ViperMonkey">https://github.com/decalage2/ViperMonkey</a>	VBA parser for analyzing malicious macros.
Exiftool	<a href="https://exiftool.org/">https://exiftool.org/</a>	Metadata analysis tool.
Bless	<a href="https://github.com/bwrsandman/Bless">https://github.com/bwrsandman/Bless</a>	Hexadecimal Editor.
GCK's File Signature Table	<a href="https://www.garykessler.net/library/file_sigs.html">https://www.garykessler.net/library/file_sigs.html</a>	File Signature table.
Message Header Field Table	<a href="https://www.iana.org/assignments/message-headers/message-headers.xhtml">https://www.iana.org/assignments/message-headers/message-headers.xhtml</a>	Table of all email header fields and information them.