Lesson 1: Phishing Analysis for Beginners

Last Update: October 2020

Introduction

Overview

This is a comprehensive guide on how to investigate phishing emails, starting at the **confirmation of a phishing event**. The goal of the resource is to support practitioners in learning and developing key phishing analysis skills so that they are able to share appropriately with other defenders and community members.

This resource is for individuals and organisations who have some technical background and are interested in practicing how to analyze phishing samples and extract data to share. Sharing indicators from a phishing sample allows us to better understand the adversary's tactics over time and develop a better sense of trends used to target at-risk groups.

Learning Goals
This is a proof of concept module based on some of the material from Internews' technical practitioner training conducted under the MONITOR project. The goal of these training sessions was to practice threat analysis and sharing in a safe way and build muscle memory to increase threat sharing among the community.

In this module you will learn the following key concepts:

- Understand the anatomy of email
- Familiarize yourself with tools to dissect an email header
- How to take robust notes during your analysis for sharing

Requirements
Before embarking on this module, it is important to remember to always handle any live malware or phishing samples with extreme caution. In this module, **there are no live or malicious emails**. This is intentional. If you desire to analyse potentially malicious threats in the future, we recommend you learn how to use and configure virtual machines for such work (not covered here at this time).

CAUTION: Like using any tool or technology, learn how it works before downloading or using anything on a device. Some of these tools require some lab setup configuration such as VirtualBox or CyberChef.

- VirusTotal
- URLScan.io
- Have i been pwned
- VirtualBox: Installing Virtual Box (Windows, Linux, Mac)
- CyberChef (do not use before reading about the tool)

Environment Setup
This cannot be overstated. Anytime you handle unknown samples be it potentially malicious files or links, you should always ensure you have the proper setup. If you're new to virtual machines, take some time to explore these resources. For real malware and phishing analysis, it is best to have a dedicated forensics machine.

Must read

[Must Read!] Operational Security

This is the most important section of this module. If you read nothing else, but only this, we will at least be somewhat satisfied. Did we mention you must handle all potentially malicious malware and phishing samples with extreme care?

Operational security is an important part of handling anything that is potentially malicious.

Resources:
- https://communitydocs.accessnow.org/252-Forensic_Handling_Data.html
- https://communitydocs.accessnow.org/258-Advanced_Threats_Triage_Workflow.html
- https://www.circl.lu/pub/tr-07/
- https://communitydocs.accessnow.org/58-Suspicious_Phishing_Email.html

Things to watch out for?

During the creation of these materials and through our own threat analysis at Internews, we are flagging some important things to be aware of when handling live phishing samples.

Automatic link creation: when someone sends you a link these days, oftentimes your messaging application will create a live link. The problem is this live link can be accidentally clicked on and therefore compromise the device you're using.

Recommendation: Clearly communicate with whomever is sending you something potentially malicious to send it to you to a location that is safe and unlikely to accidentally click or preview.

Content preview: Similarly, many messaging services will now give you a preview of a live link by default.

Recommendation: Clearly communicating with the sender is important. Do not have them send links over messaging apps unless they know how to defang or have content previews turned off. Failure to do so could potentially compromise you both.

Beacon URLs: These URLs automatically "phone home" to a control server operated by the adversary and can send valuable information to the attacker such as the email has been opened at this IP address, at this time and date, in this browser -- all of which allow for further tailoring future attacks against the community.

Recommendation: Ensure you have disabled auto-loading of external content so beacon URLs are not automatically triggered.

Important Considerations Before Submitting URLs to Services like VirusTotal.

Before submitting any potentially sensitive data to an online service, it is important to think about the repercussions or consequences of using the service in question. Why? Well because these services are run by companies and people and anything you upload should be considered shared with them.

For example, tools like VirusTotal are actually run and operated by Google and Have I Been Pwned is run by an individual named Troy Hunt.

Virustotal origin (Google product)

How to visit a URL safely?

When visiting a potentially malicious URL, it is important to not visit directly unless you've spent time setting up and configuring your lab environment. **This is critical so that you do not accidentally download malware onto your device.**

Cuckoo Sandbox: If you have access to a sandbox environment like Cuckoo you can use the sandbox to do further research in a safe environment,

Unshorten URL: In some instances, the adversary may attempt to obfuscate the URL destination by using what are called "URL shorteners". To deobfuscate, the practitioner should carefully use an unshortener service and "defang" the URL immediately.

Phishing

Types of phishing

Phishing can come in a variety of types, but the most frequent we've seen in our work is either:

- Phishing with a malicious link
- Phishing with a malicious attachment / file

Commodity Phishing vs Targeted Phishing

	Commodity phishing	Targeted phishing
Motivation	Financial gain, Recognition	Power, Political, Financial gain
Resources	Hacker, script kiddie	Hacker groups, State agencies, multi-national companies
Targets	Targeting multiple persons at once, not interested in their profile	Targeting a specific person or a group of persons due to their work
Risk	Loss of data, money	Reputation harm, arrestation, physical integrity harm

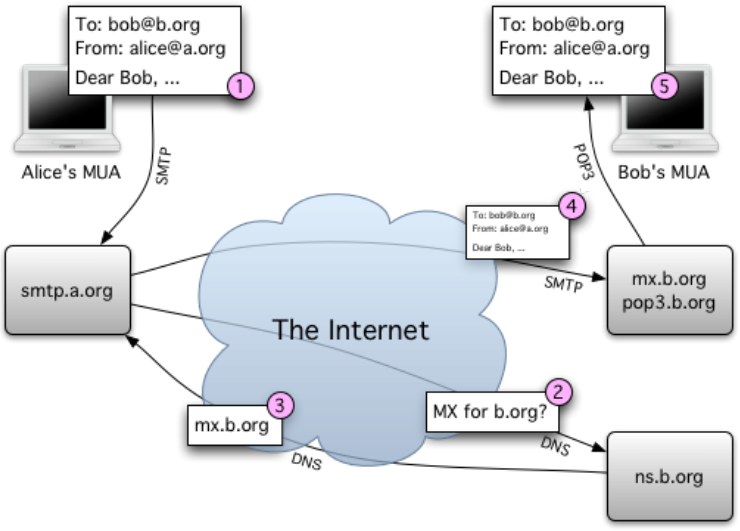
    - Caveat, simply because it is targeted does not necessarily mean a nation-state. We've seen criminal groups also conduct targeted attacks.
        - Human operated ransomware : link
- Examples of targeted nation state phishing attacks
    - German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed (2020): link
    - Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools (2020): link
    - Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries (2018): link

Essential concepts

How email works?

WHAT IS SMTP?

SMTP is a simple text based protocol that stands for Simple Mail Transfer Protocol. It is the standard technology used when sending email.



https://upload.wikimedia.org/wikipedia/commons/9/96/How_e-mail_works.png

1- The user writes an email and an SMTP request is initiated
2- A request is sent to the DNS server to identify the recipient Mail Transfer Agent (MTA).
3- The MX record is identified
4- The email is sent to the recipient MTA
5- The email is delivered to the recipient

Below is how an SMTP session would occurs :

C: telnet mysmtp.com 25	Contact the server on port 25
S: 220 mysmtp.com ESMTP Exim	The server is ready to start the email communication
C: HELO mydomain.com S: 250 Hello mydomain.com	HELO message initiate the communication and the server is ready to receive email commands.
C: MAIL FROM:<sender@mydomain.com> S: 250 Ok C: RCPT TO:<recipient@anotherdomain.com> S: 250 Accepted	Both sender and receiver are mentioned and the server is responding with an okay message.
C: Data S: 354 Enter message, ending with "." on a line by itself C: Subject: sample message C: From: sender@mydomain.com C: To: recipient@anotherdomain.com C: C: Greetings, C: Typed message (content) C: Goodbye. C: . S: 250 OK	Initiate transmission Informing about the closing character The message is send by the client ending by the closing character mentioned above. The email was received successfully

C: QUIT S: 221 www.sample.com closing connection	End of session Connection closure

Other Recommended Readings:

- https://www.smtp2go.com/blog/understanding-smtp-protocol/

What is a DNS?

DNS stands for Domain Name System. It basically returns back the exact IP address of a server by having its domain name.

What is an MX record?

It is a record that can be found in DNS servers. It is essential for email delivery. MX records consist of two parts: the priority and the domain name. For example:

1 mail.mywebsite.com

- 1 is the priority
- Mail.mywebsite.com is the email server

Dissection of an email header

Dissecting an Email Header

This section dissects an email header or the raw email data.

- SPF Record
- Final Received
- Mime Boundary
- Decoding Subject
- Email Encoded Text

Parts of an Email

[pull out specific header fields and write definitions that would be important; note which things can be spoofed]

- **Fromf**
- **Sender**
- **Date**
- **Received SPF**

- **X Originating IP**

The easiest way for finding the original sender is by looking for the X-Originating-IP header. This header is important since it tells you the IP address of the computer that had sent the email. If you cannot find the X-Originating-IP header, then you will have to sift through the Received headers to find the sender's IP address.

Email Header Fields

From: =?UTF-8?B?2onbjNixINqJ24zYsSDYqNivINiz2pPbjA==?= <badguy@gmail.com>
Email Address: badguy@gmail.com
Name Display: ویر ویر بد ولین
Translated Display Name: Very Very Bad Villain
Encoded Display Name: =?UTF-8?B?2onbjNixINqJ24zYsSDYqNivINiz2pPbjA==?=

Decoding Subject

=?utf-8?Q?=E9=87=8D=E8=A6=81=E6=96=87=E4=BB=B6?=

Email Encoded Text

=?charset?encoding?encoded-text?=

Received Sender Policy Framework (SPF)

The Sender Policy Framework (SPF) is an email authentication technique that is used against email spoofing. Setting up an SPF record helps to prevent malicious persons from using your domain to send unauthorized (malicious) emails, also called email spoofing. The SPF protocol is

used as one of the standard methods to fight against spam and is also used in the DMARC specification.

Received-SPF: Fail (protection.outlook.com: domain of newpaltz.k12.ny.us does not designate 67.231.149.212 as permitted sender) receiver=protection.outlook.com; client-ip=67.231.149.212; helo=mx0a-0006f202.pphosted.com;

MIME Boundary

Content-Type:multipart/related;boundary="==========1234567890123456789=="

Final Received

Received: from nsr.server2.gr (nsr3.server2.gr [78.47.58.124]) by Vanessa.inwise.de (amavisd-milter) with ESMTP id 05GASOLK001698; Tue, 26 May 2020 13:09:49 +0200

(envelope-from <administracion@serlingo.es>)

Mailer and User Agent

X-Mailer: IBM Notes Release 9.0.1FP5 SHF237 March 19, 2016

The sender used IBM released Lotus Notes/Domino 9.0.1 FP5 to send the email.

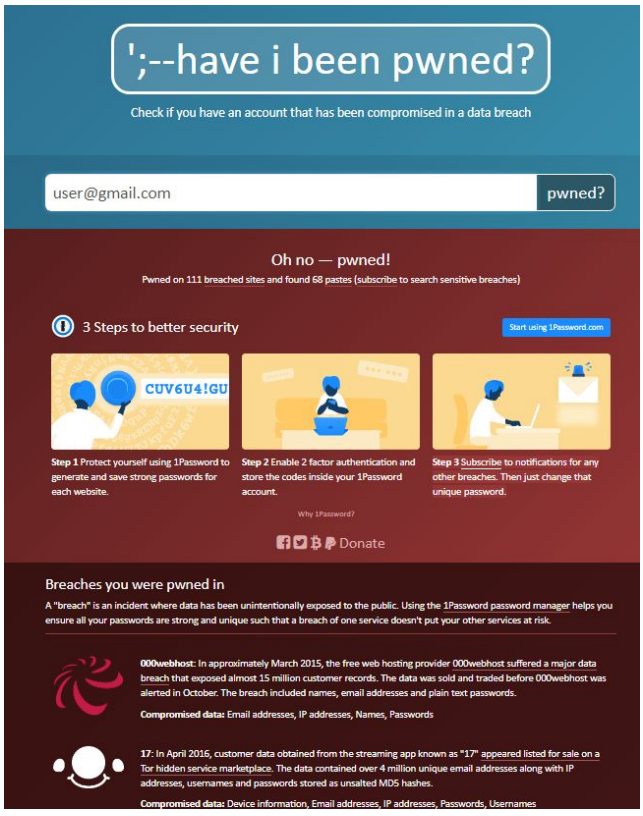
Useful tools

Useful Tools

VirusTotal: www.virustotal.com

It is an online resource on which you can scan malicious files and links.The website will scan what you provided to it and check it over 50 security tools databases. If a malicious activity is detected, you will be notified. You can scan suspicious files by downloading them from the phishing email and upload them on Virustotal and make sure to not run them on your computer. You can copy/paste the source of the link you received on the phishing email without accessing it.

HaveIBeenPwned:https://haveibeenpwned.com/

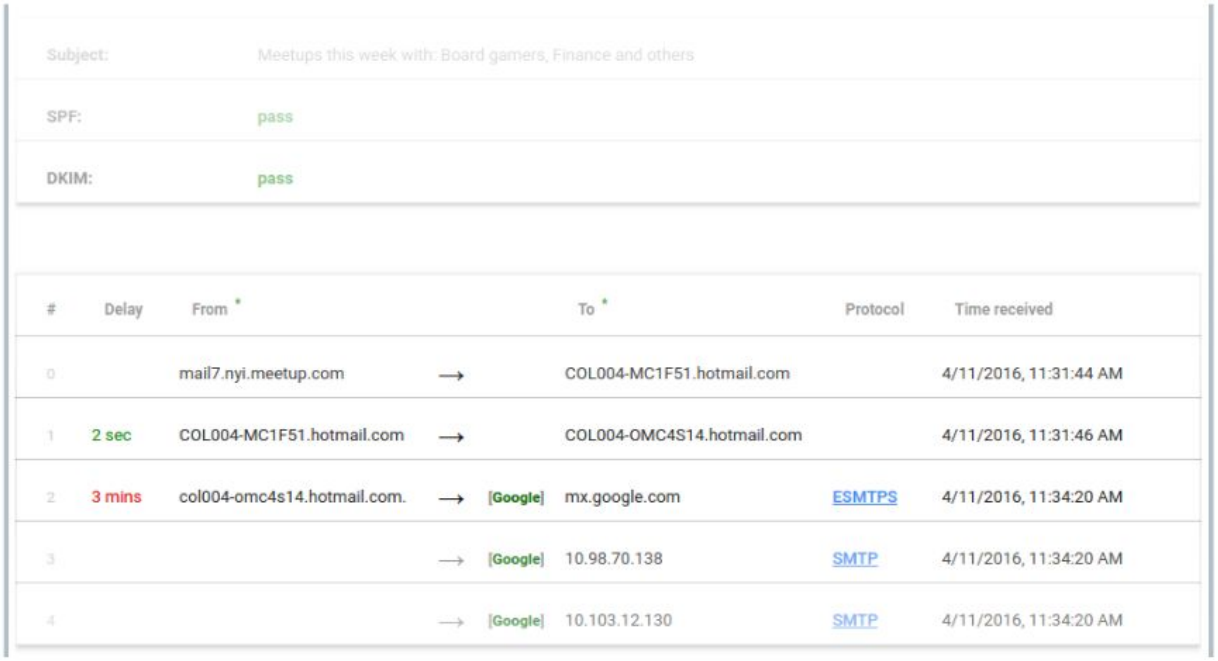


It is a free online resource that allows you to fill an email address and check if it was subject to known data breaches by searching databases. This will help you know if the email address you are using or the email address you are interacting with is potentially compromised.

Google Admin Toolbox

This is the most practical tool when we are talking about headers analysis. In fact, you will need to copy the headers of the email and paste it in the Google Admin Toolbox. Google will analyse the headers for you and notify you if there are any inconsistencies.

https://toolbox.googleapps.com/apps/messageheader/?lang=en



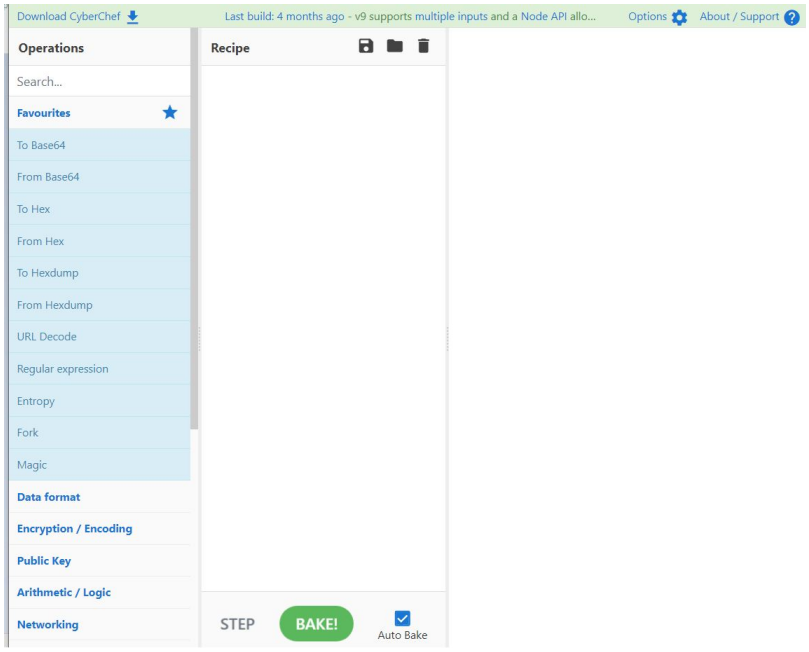
Subject:	Meetups this week with: Board gamers, Finance and others
SPF:	pass
DKIM:	pass

#	Delay	From *		To *	Protocol	Time received
0		mail7.nyi.meetup.com	→	COL004-MC1F51.hotmail.com		4/11/2016, 11:31:44 AM
1	2 sec	COL004-MC1F51.hotmail.com	→	COL004-OMC4S14.hotmail.com		4/11/2016, 11:31:46 AM
2	3 mins	col004-omc4s14.hotmail.com.	→ [Google]	mx.google.com	ESMTPS	4/11/2016, 11:34:20 AM
3			→ [Google]	10.98.70.138	SMTP	4/11/2016, 11:34:20 AM
4			→ [Google]	10.103.12.130	SMTP	4/11/2016, 11:34:20 AM

CyberChef

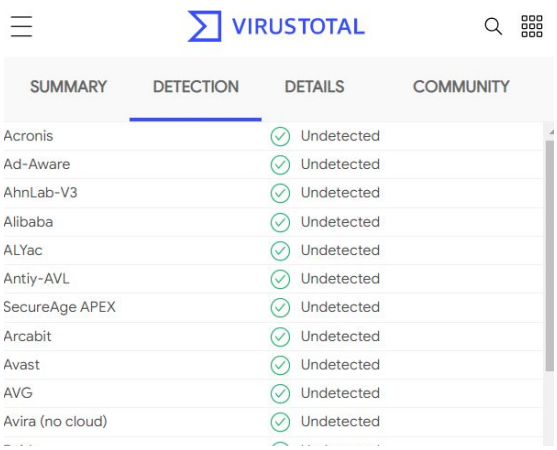
CyberChef is a tool we would only ever suggest using on a virtual machine.

- CyberChef: Parsing and Formatting
- CyberChef: Recipe Sharing
- Open source, GCHQ created



URLscan.io

- Has the email address been compromised?
  - Resource: https://haveibeenpwned.com/



VirtualBox

VirtualBox is a free virtual machine that contains a mini version of a live operating system. Virtual machines are an important tool in analysing potentially malicious files and emails so that you do not accidentally infect your host machine. An added benefit of using virtual machines like VirtualBox is that you can take a snapshot of the machine and reinstate it if something goes wrong.

Note taking

[Must Read!] Note Taking

Now you may be thinking, what is note taking doing in this module. However, note taking and organization are critical pieces of threat analysis. The goal should be creating a document that is clear, easy to read, and potentially actionable for another researcher.

- Methodical and careful note taking during threat analysis is critical to rigorous and thorough
- “Defang” everything, always!
- Note taking sample template
- Take special care to note these things:
  - SPF Record
  - Final Received

        - Mime Boundary
        - Decoding Subject
        - Email Encoded Text
    - Screenshots: ensure you know how to do screen shots
    - Report writing
        - [1] Lenny Zeltser, "*Top 10 Cybersecurity Writing Mistakes*"

Online Lecture Materials

- SMTP protocol : link
- Locate email headers : link
- Understand email headers: link
- Malware analysis via Virtualbox : link
- Phishing example : link
- Preventing from malware : link

Practice

Exercise

The objective of this exercise is for the student to analyse a normal email header and be able to identify the different types of data, collect them, and organize them in a concise report to share.

- Upload benign email header (.eml file)
- Specific tasks to complete
    - *Locate the From and Return-Path email addresses*

        - *Are they similar?*
        - *What can you tell?*
    - *Specify the same of the sending server machine*
    - *Where is the sending machine located?*
    - *Are there any malicious links / attachments in the message?*
        - *How would you analyze them?*
        - *What did you find?*
    - *Does this email represent a phishing attempt?*

- Link to pdf with results