Automated Collection With PhishTool

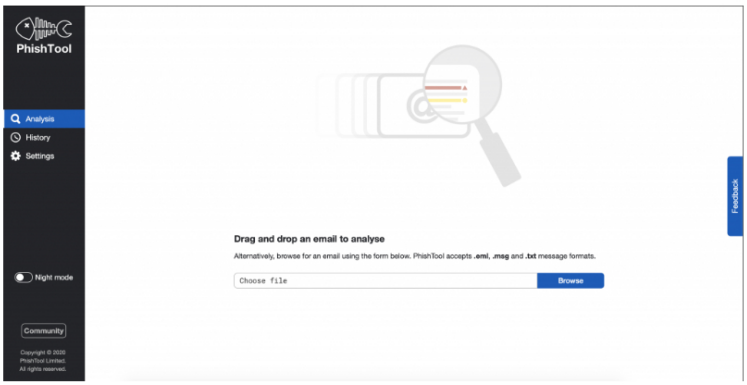
PhishTool provides a forensic analysis console, giving individuals the power to forensically analyze phishing emails, tag malicious artifacts, and generate investigation reports. This incredible platform can do all the heavy-lifting in terms of artifact retrieval and even artifact analysis. This lesson will walk you through how to use the platform to upload phishing emails and generate reports.

ACCOUNT REGISTRATION

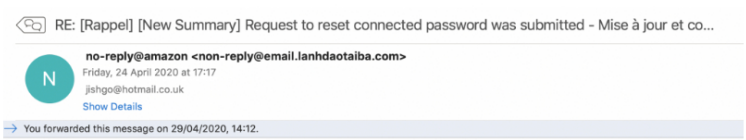
You can register for a free Community Edition account over at https://phishtool.com. These accounts have a limit on the amount of emails that can be analyzed – but thanks to the great guys at PhishTool, all email FILES included in Blue Team Level 1 have been whitelisted, meaning they will not use up your monthly analysis allowance!

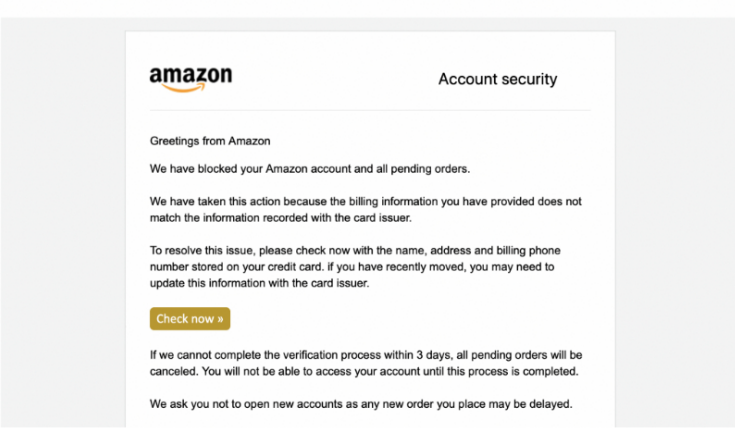
EXAMPLE ONE

On the analysis console homepage, you'll be presented with the view as shown in the below screenshot. This is where we can drag-and-drop a malicious email, or browse of file system and upload it.

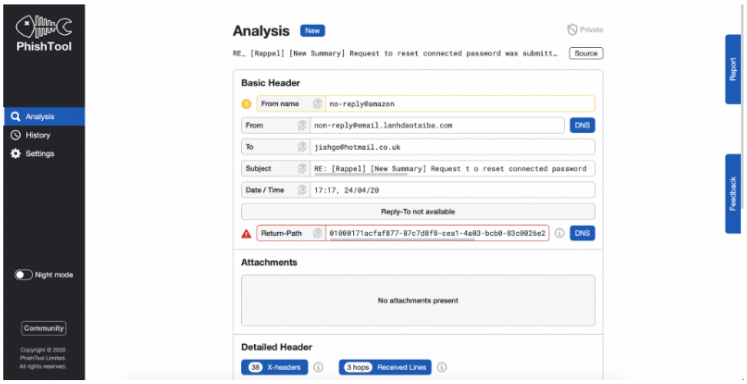


In this case, we're going to click the Browse button and find the email we want to submit for analysis. In this case, we're going to upload this Amazon credential harvester!





Once the analysis has completed, you will see a screen that looks similar to the following screenshot. This page holds all of the results from artifact extraction and analysis procedures. Whilst there is a ton of useful information we can retrieve and fun things we can do, for the scope of this lesson, we are only interested in retrieving artifacts from the email (don't worry, you'll be using PhishTool later for analysis tasks!). You can click the clipboard icon next to artifact names to copy them.



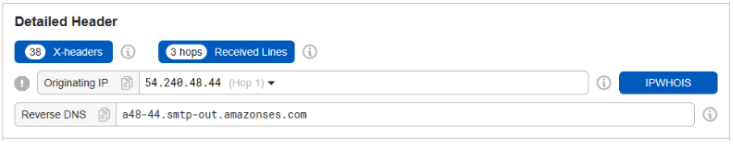
The artifacts we're interested in are:

1. **Sending Address**
2. **Subject Line**
3. **Recipients**
4. **Date + Time**
5. **Sending Server IP**
6. **Reverse DNS**
7. **URLs** (if applicable)
8. **File Name** (not applicable)
9. **File Hash** (not applicable)

So let's gather these from the PhishTool analysis console! In this **Basic Header** section, we will be able to retrieve artifacts **1, 2, 3, and 4.**

Below this there is a section for **Detailed Header** that includes the X-Originating-IP and the reverse DNS results

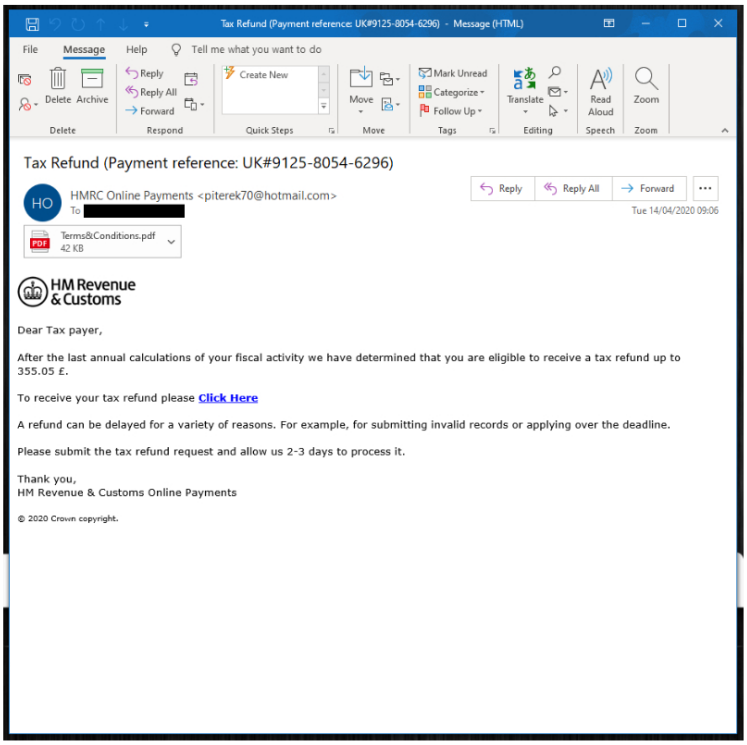
Below this there is a section for **Detailed Header** that includes the X-Originating-IP and the reverse DNS results, which gives us artifacts 5 and 6.



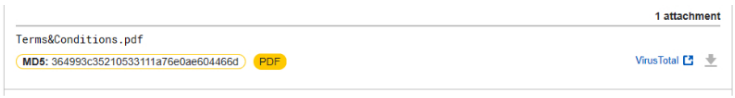
And finally down at the bottom we have a section for **URLs**, where we can retrieve all hyperlinks that were included in the email.

EXAMPLE TWO

In this second example we're going to submit an email that has a potentially malicious attachment, so we can show you how to retrieve file-based artifacts using PhishTool. Below is a screenshot of the phishing email we're going to analyze.



After submitting the email to PhishTool, under the Basic Header section there is a section titled **Attachments**. This provides us with the MD5 hash of the file, and the file name! We can also click on the VirusTotal link to automatically submit the hash for analysis and retrieve a community reputation score.



CONCLUSION

This lesson has shown that it is able to retrieve email, web, and file-based artifacts all from within the PhishTool Analysis Workbench, making it a faster alternative to manual collection. It is still extremely important to know how to collect indicators manually using a client and text editor, in case you don't have access to PhishTool, such as when investigating analysts do not have an internet connection.

Previous Topic
Back to Lesson
Next Topic