[Video] Collecting Artifacts – Automated Methods

Transcript

In this video, we'll be using PhishTool to quickly gather email, web, and file-based artifacts from suspicious emails. For the first example, we'll be using the email from the previous video where we gathered artifacts manually using an email client and a text editor. This is the HMRC tax refund themed credential harvester with the malicious URL and a PDF attachment.

Let's open our browser and visit phishtool.com. PhishTool is a forensic-grade email analysis platform that allows us to upload emails and retrieve lots of useful information that will let us investigate it further. Once we've logged in it'll take us to the analysis console. On this page, I can either upload the email file directly, or just drag-and-drop into the console. Here you can see we're presented with lots of information, but for the scope of this video, we're only interested in retrieving the important artifacts. So at the top we have the sending address, the recipient which is the email honeypot we're running, the subject line, the date and the time, and the return path where the email replies will be sent. We can actually copy these values quickly just by clicking on the clipboard icon next to the value.

Below the email artifacts, we also have the file artifacts, in this case the file name and the MD5 hash value. Next, we have the sending IP address, also known as the originating IP address, which belongs to the sending server. And finally, at the bottom we have the web artifacts, with the malicious URL down at the bottom. So it's a lot faster to retrieve artifacts if you have access to PhishTool. It can also perform artifact analysis and other investigational activities, but we'll cover that in a future video.

Now let's try another suspicious email that is posing as an Amazon security alert. We can see that this email has pretty poor styling, the branding images aren't available at time of analysis, and it's enticing the recipient to click on a button, so we can assume with good

confidence that this is another credential harvester trying to steal Amazon credentials. Hovering over the button we can see that this directs to theboozebakery[.]com which obviously isn't Amazon.

Let's drag this email into the analysis console, and again we can quickly retrieve the sending address, the recipient, the subject, the date and time, the return path, the originating IP address, and the URL down the bottom. One extremely useful feature that PhishTool offers is the ability to generate reports based on the information collected from an email. Clicking on the report tab on the right will allow us to generate a plain-text or pdf report if we tag at least one artefact. Let's go ahead and tag the sending address and see what a plain text report looks like. It will copy our information to a clipboard, so lets paste it into an empty notepad. We can see that we have all the information from the analysis console, now in a basic text format, so we have our own record of the artifacts, such as the sender, recipient, subject, date, return path, as well as file-based and web-based artifacts.

Now let's show you the PDF version of the generated report. PhishTool will offer us a nicely-styled report that includes all of the information we need, and it's very easy to read. So PhishTool definitely makes the job of retrieving artefacts easier and quicker, and it can provide us with neat reports that we can keep for future reference.

Previous Topic
Back to Lesson
Next Lesson