[Video] Collecting Artifacts – Manual Methods

Transcript

Hi everyone, this is John here. This video is going to focus on retrieving email, web, and file-based artifacts from a suspicious email. The email we're looking at here in the Thunderbird client is a phishing email that is posing as HM Revenue and Customs, or HMRC. There's immediately a number of red flags, such as;

Opening says "tax payer" instead of the recipient's name

The pound symbol is after the amount

The copyright text at the bottom looks dodgy

And the email is styled pretty poorly.

Let's quickly recap on the artifacts we need to gather from the email.

We can find the sending address at the top

Below that we have the subject line

The date the email was sent is in the top right

Then we also have a URL that is hyperlinked to the text here, and there's actually a .pdf attached too.

There's another artifact we need to collect here, and that's the sending server IP. So I'll right-click the .eml file, and open it using Sublime Text 2.

So if we search for "subject" we can see all of the information we just gathered in text format. We have:

The sending address

The recipient, which we've changed in this example

The subject line

And the date

Now if we search for "sender" we'll get taken to the x-Sender-IP value, which is 40.92.90.99. We also need to know the reverse DNS of this IP address so we can see where the email actually came from. I'll copy the IP, and load up Domain Tools to perform a WHOis lookup. Once we paste the IP in, we'll get a ton of valuable information about that host. In this case, the hostname ends in outlook.com, which tells us that this is a Microsoft-owned email server for Outlook, and that the email has originated in Outlook. All the information down here is just contact details for various Microsoft teams.

Next, we need to retrieve any web artifacts, in this case the URL from the email. If we go back to our text editor we can search for "http" which will highlight any http or https URLs for us. We can see that this section here is actually the body content of the email, and we have the likely malicious URL here in "a" tags, so we want to note this down, giving us the URL and the domain name.

Then finally we have file artefacts. We saw earlier that there was a PDF with this email. So you can either click save as, as shown here in Outlook, or just drag and drop to our desktop. Make sure not to run the file at ANY POINT. We're on a Windows host here so we will hold [Shift] and right-click and open a PowerShell window, or you can do this by going to the start menu and searching for PowerShell. We want to retrieve the hashes for this file. Typically we only want the MD5 hash value, but in this example, we'll get the MD5, SHA256, and SHA1 values. We want to use the get-filehash command, start typing the name of the file, so "T E R M S" and press [Tab] to autofill the file name. When we hit enter, by default this command will give us the sha256 value. To get the MD5 and SHA1 values we'll use the same command, but use the algorithm switch to choose the hash type, and we'll use a semi-colon to chain the commands together so we don't have to do them separately. A couple more artefacts we want can be found by right-clicking the file and going to properties. We want the file name and the file size. This has been a video on manually retrieving email, web, and file-based artefacts from a suspicious email.

Previous Topic
Back to Lesson
Next Topic