[Video] Manual Artifact Analysis

Transcript

In this video, we're going to cover how to analyse artifacts retrieved from a suspicious email to get a better understand if the email is malicious. The email we are analysing in this example is an email that is impersonating PayPal with some pretty basic styling and is using a hyperlink lure to get recipients to visit a URL.

We have already collected the artifacts from this email so we can begin the analysis stage. This email does not include an attachment so we are going to focus purely on the URL. First things first, let's upload the URL to VirusTotal to do some initial reputation checks. Immediately we can see that six engines are flagging this URL for malicious purposes or phishing. In the top right, we can see that it was first uploaded 4 hours ago and it has a HTTP status code of 200, meaning that it is still available on the internet.

Now let's take a look at what is actually on that URL using URL2PNG. This is pretty strange – we were expecting to see a credential harvester for PayPal, but this just looks like a ton of encoded data. To get a better look we can right-click the image pane, go to Inspect Element, and copy the img id sample URL and paste this into a new browser tab. So this specific URL is hosting a lot of encoded data, which most likely is malware, but first, we should do some more checks.

We can enter the URL into the WHOIS lookup by Domain Tools to get more information on the domain. It says here that the site has been alive for 299 days. If the page was created a few days ago, then I would start to think it was created purely for malicious purposes, but in this case, it may be a legitimate site that has been compromised.

To see if the site is legitimate, let's go back to URL2PNG and only search for the root domain, surroundsound[.]in. It looks like it is just a white page, so either the homepage

isn't loading correctly, or there's simply no content there, which isn't something a legitimate website would have.

Let's visit wannabrowser.net and search for the root domain to see what HTTP response code is returned. This responds with a 500 code internal server error. This is a generic error and means the server can't fulfill the request to load the homepage. Let's try the full URL. Again we're presented with the encoded data, and there's loads of it.

Let's head over to the hybrid analysis so we can see if this is really malware. We can paste the URL into the file or URL tab and click analyse. We just need to confirm that we're happy for the report to be public, and we agree to the terms and conditions. So click continue and select our virtual machine, we'll stick with the default Windows one. At the moment there are 16 other requests in the queue, so I'll fast forward to when the report is done. Now we can see the URL has been flagged as malicious, with a score of 50/100. So let's open up the full sandbox report. The malicious indicators are that this URL has been flagged by anti-virus engines. At the top we are able to see the MITRE ATT&CK Framework TTPs or the tactics techniques and procedures that have been identified. We will cover the MITRE ATT&CK Framework and go more in-depth on these TTPs in the Threat Intelligence Domain later on.

One last place that I like to search for likely malicious URLs is URLHaus, or h-a-u-s. We can upload the URL via the database and see if anything comes back. It looks like this URL has been flagged for hosting an encoded version of the AveMairaR-A-T or RAT, for remote access trojan. So we now have confirmed malware! Just going back to URL2PNG we can see that all of this encoded data is actually a remote access trojan.

Now we have analysed the artifacts and confirmed that this email is extremely malicious, and can download malware to a victim's system.

Previous Topic
Back to Lesson
Next Topic