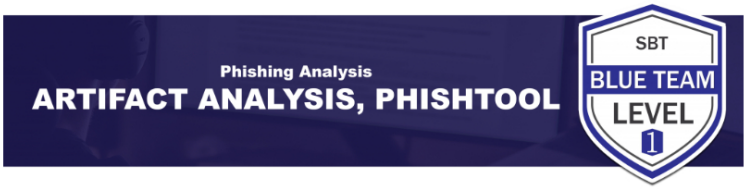
[Video] Artifact Analysis with PhishTool



Transcript

In this video, we're going to cover how you can analyze artifacts directly from the PhishTool analysis console. We're going to stick with our previous email example, the HMRC credential harvester that has a PDF attachment and a malicious URL. Let's go ahead and open up PhishTool, login, and drag the email into the analysis console.

First, we'll look at the PDF, and we have been provided with the MD5 hash value. If we click on the "VirusTotal" link to the right-hand side PhishTool will generate a search query for the MD5 hash and take us to the report page so we can perform a quick reputation check and see whether the security community has marked this file as malicious or not.

We can see that no engines have detected this file as malicious, which could suggest that the file is harmless. At the top we have the file name, the hash, the size, and when it was first submitted. As this file hasn't been reported as malicious, it's potentially just a PDF with text inside. We can open this inside a snapshotted VM. In this case, we're using a Kali VM. So we'll drag the PDF into our VM, disconnect from the network in case there's any nasty surprised inside that attempt to call out and download other files, and open the PDF. We can see this is just a basic PDF with text content that is trying to make the whole email appear more convincing by creating this fake government documentation.

Next, we want to analyze the URL that was included in the email. If we click on the URL at the bottom of the analysis console we can perform two actions, a web capture, and a WHOIS lookup. Let's start with the web capture so see what's on this URL. From the capture, we can see that whatever was previously here has been taken down, likely by the site owners. In the bottom section, we're also able to view the headers from the URL request, and the HTTP request on the left-hand side.

Doing a WHOis lookup will give us information about the domain. The first thing that

stands out is that this domain has been in use for 2835 days which shows that the domain is likely legitimate, and isn't newly-created for malicious purposes. Combine this with the fact that the page is no longer available, it is likely that this is a legitimate website which was compromised to host a credential harvester, which the site admin has since removed.

Since we checked the file MD5 hash in VirusTotal, we should also check the URL to see if it has been recognized as malicious. We can copy the URL by clicking the clipboard icon, going to VirusTotal.com, and searching for it under the URL heading. Again there have been no engines flagging this URL as malicious. We can also double check the root domain by removing the URL ending, and this too comes back with no negative reputation, backing up our theory this is a legitimate domain that was temporarily compromised but fixed by the site owners.

Previous Topic
Back to Lesson
Next Lesson