Analysis Process, Tools, and Results

This section will be the largest part of your report, and will cover the analysis you completed to assess the risk of any malicious artifacts such as attachments or URLs. You will include the tools you have used, and the results that they have provided. This can include visualization tools, reputation check results, as well as manual investigation methods such as detonating malware in a virtual sandbox.

I have split this lesson into two parts: URL analysis, and attachment analysis. This will show you how to write Section 2 for either occurrence.

EXAMPLE ONE

Malicious Artifact Analysis (URL) Report Example

- **URLs:** http://maliciousdomainexample[.]com/index/2019/amazon/login.aspx
  (*The following analysis is not reflective of this URL, but is based on previous experience in investigating phishing emails and sites, and therefore reflects real investigations*).

WHOIS Analysis – Performing a WHOIS search shows that the domain was registered 3 days ago, with NameCheap as the domain registrar. There is no information about the site owner/domain registrant.

VirusTotal Reputation – Searching for the full URL and the root domain on VT show that it is currently not being flagged as malicious, likely the result of the domain being new, so security engines haven't crawled it yet.

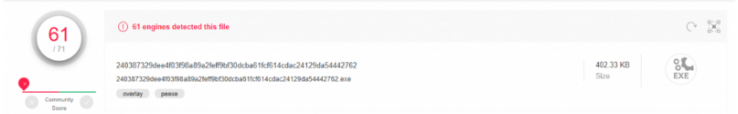
URL2PNG Analysis – Using URL2PNG to view the link destination showed that the site was hosting a fake Amazon login portal, used to steal any credentials that are entered. Looking at the root domain "http://maliciousdomainexample[.]com" shows that the site doesn't have a genuine homepage, a common sight when domains are used for purely malicious operation.

EXAMPLE TWO

Malicious Artifact Analysis (Attachment) Report Example

- **Attachment Name:** wallpaperHD.exe
- **Attachment MD5 Hash:** 0c4374d72e166f15acdfe44e9398d026
- **Attachment SHA256 Hash:** 240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762

VirusTotal Upload – Uploading the file to VirusTotal shows that the file is extremely malicious and is detected by 61/71 engines. Link to VirusTotal page for this MD5 hash – https://www.virustotal.com/gui/file/240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762/detection



Talos File Reputation – Uploading the SHA256 hash to TFR confirmed what VirusTotal stated about the file being extremely malicious.

CONCLUSION

This is going to be the most detailed part of your report, as this is where you actually assess the risk of malicious artifacts to the organization. You need to answer questions such as "is this URL malicious?" or "how damaging is this attachment?" whilst providing in-depth notes on the analysis methods and tools you used to investigate these artifacts. This section will later provide justification for any defensive measures that you wish to take, so there needs to be enough detail to allow senior analysts to come to the same conclusion that you have. In the next lesson, you will be given a chance to write your own Section 2 as practice before the final assessment.

Previous Topic
Mark Complete
Next Topic
Back to Lesson