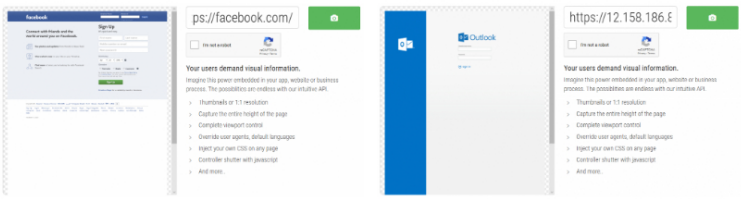
Visualization Tools

This lesson will cover tools we can use to visualize a malicious URL without actually having to visit the site, as it could be highly malicious. The tools we're going to cover are URL2PNG, and URLScan. By the end of this lesson, you will feel comfortable with visualizing hyperlinks to assess what is on the other side.

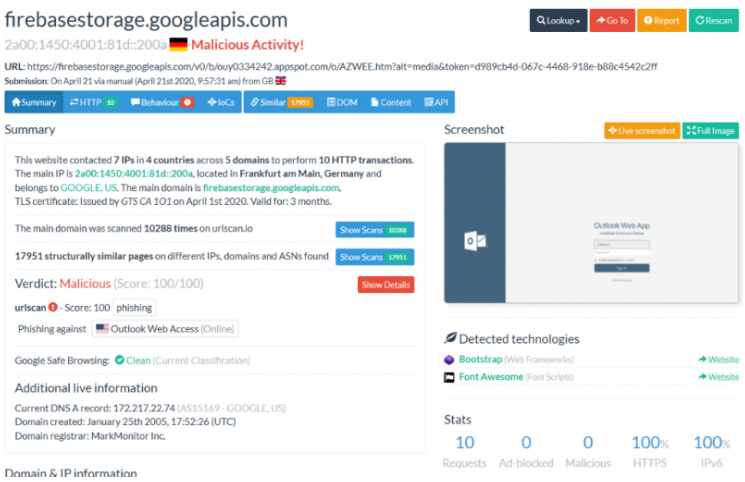
URL2PNG

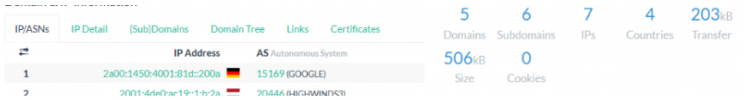
URL2PNG is my go-to tool for visualization. You simply enter in a URL, hit go, and it'll provide you with a screenshot of what the webpage looks like. Let's go through a couple of examples. The screenshot on the left shows me entering the following URL into URL2PNG: https://facebook.com/. The screenshot on the right shows me entering a malicious URL for a real-world Outlook Web Access credential harvester into the tool:



URLSCAN

URLScan, amongst other information this tool gathers on a searched URL, has the ability to provide a screenshot. In this example, you can see a screenshot has been taken on the right-hand side, allowing us to see what the destination web page looks like. In this case, it is an Outlook Web App credential harvester.





CONCLUSION

Visualization tools are key to allowing analysts to identify what is on the other end of a hyperlink without having to visit the page directly. Whilst it is not necessary to include a screenshot of the destination in your investigation report, it's something I like to do!

Previous Topic
Back to Lesson
Next Topic