Report Challenge 1

Alexandru-Mihai Crusninschi (s3339688)

Andrei Ursachi (s3351912)

- *Questions 1*

  We can successfully hide everything that appears in the header, in this case we are mainly interested in the UserAgent, which we successfully modified. The IP cannot be hidden because it is part of the fundamental design of the transport layer, specifically the TCP/IP protocol.

- Questions 2

  A lot of these domains are used to collect data from the user accessing the initial URL. They are used for monetary gains as a lot of them corresponds to ads. The URL containing a lot of information is actually a text file that serves as a log for all user interactions and metadata generated by the browser.

- *Questions 3*

  Lots of these urls are used for data metrics and metadata analysis. Around 50-80, just a guess. Yes, there is a website that occasionally pings the connection. The ping website is also the one who keeps track of when the tab was closed.

- *Questions 4*
  A lot can be done to improve online privacy and the list includes things like using a hardened web browser, disabling as many malicious connections as possible, disabling javascript and using privacy respecting platforms. Of course, things like disabling javascript would result in the user being unable browse a lot the popular platforms these days (SPAs). Since the extension is very bare bones it doesn’t break anything yet, except maybe for some misbehaving canvas elements due to dynamic rendering.

Observations and code inspection

We have observed that depending on which site we click on there are a number of additional requests that the website makes on our behave, acting as a proxy to analytics, tracking etc. In order to mitigate this, what our code is doing is the following, just before the request is sent, we parse the request URL and if the following keywords are present we cancel the request: analytics, ads, amazon, metrics, ping, privacy, logs, optimizely. In addition we change our user-agent to “None of your bussiness”.