Alex Miller

Security, Privacy, and Consumer Protection: Lab3

Chosen Website: https://thisiswhyimbroke.com

(1) Capture the DNS queries made by your browser when loading this website. You can do this either with a tool like wireshark. Please include your results in the form of a pcap that contains *only* the DNS queries (you can filter for DNS queries in Wireshark). Based on your data:

- *Who (i.e., what companies) can see that you've visited the website based on unencrypted DNS queries?*
    - My ISP, when I query their recursive resolver
    - Potentially any other ISP or network provider my ISP has a traffic sharing agreement with, if I'm using a non-default recursive resolver
    - The operators of any such DNS recursive resolver
- *Beyond DNS queries, name all other entities that know you've visited the website. Present your findings by grouping your domain names into companies (e.g., the company "Google" has many domain names). Explain how these companies may have visited the website. What different types of concerns might you have about the above companies knowing this information (concerns may differ by company!).*

  I first navigated to https://thisiswhyimbroke.com, and then clicked on the following listing. This triggered the following DNS queries, due to the webpages served to me requesting additional assets, resources, and services using embedded JavaScript, or due to my browser attempting to perform related tasks, such as validating SSL certificates.

    - AGKN Advertising
        - Domains:
            - d.agkn.com
        - Concerns:
            - Data provided by either webpage I visited can give this advertiser information on how to track me across the web, and deliver me content I will engage with
    - AWIN
        - Domains:
            - www.awin1.com
        - Concerns:
            - Data provided by either webpage I visited can give this advertiser information on how to track me across the web, and deliver me content I will engage with
    - Bing
        - Domains:
            - Bat.bing.com
        - Concerns:

Commented [AM1]: Some sort of JS tracker

        - Data provided by either webpage I visited can give this advertiser information on how to track me across the web, and deliver me content I will engage with
- Etsy
    - Domains:
        - www.etsy.com
        - i.etsystatic.com
    - Concerns:
        - Etsy was hosting the posting for the product I clicked on. They might share secure information with other companies after I've established a connection with their servers.
- Facebook
    - Domains:
        - star-mini.c10r.facebook.com
        - www.facebook.com
        - Connect.facebook.net
    - Concerns:
        - Facebook can use the fact that I visited either ThisIsWhyImBroke or Etsy to suggest products and services to me, and build a picture of what types of things I want to buy.
- Google
    - Domains:
        - adservice.google.com
        - analytics.google.com
        - www-googletagmanager.l.google.com
        - partner.googleadservices.com
        - fonts.googleapis.com
        - safebrowsing.googleapis.com
        - pagead2.googlesyndication.com
        - tpc.googlesyndication.com
        - www.googletagservices.com
        - Ocsp.pki.goog
        - us-central1-adaptive-growth.cloudfunctions.net
        - encrypted-tbn0.gstatic.com
        - fonts.gstatic.com
        - www.gstatic.com
        - 8666735.fls.doubleclick.net
        - 9910951.fls.doubleclick.net
        - googleads.g.doubleclick.net
        - googleads4.g.doubleclick.net
        - Stats.g.doubleclick.net
        - S0.2mdn.net
    - Concerns:

        - Google can sell the knowledge that I visited ThisIsWhyImBroke or Etsy to other entities, or build an ad profile for me themselves in order to suggest content on their platforms.
- Granify
    - Domains:
        - cdn.granify.com
        - Matching.granify.com
    - Concerns
        - This indicates that Etsy is using Granify in order to drive my product engagement, and improve sales for Etsy retailers.
- Pinterest
    - Domains:
        - s.pinimg.com
        - Ct.pinterest.com
    - Concerns:
        - Pinterest now knows more about what sort of products I want, and can better serve my engaging content.
- Survata
    - Domains:
        - ir.surveywall-api.survata.com
    - Concerns:
        - ThisIsWhyImBroke is using this marketing analytics tool in order to improve their listings and ad placement
- ThisIsWhyImBroke.com
    - Domains:
        - thisiswhyimbroke.com
        - cdn.thisiswhyimbroke.com
        - www.thisiswhyimbroke.com
    - Concerns:
        - ThisIsWhyImBroke was hosting the listing for the product I clicked on. They might share secure information with other companies after I've established a connection with their servers.
- Xg4ken
    - Domains:
        - Resources.xg4ken.com
    - Concerns:
        - This is a known (possibly malicious) browser tracker associated with malware use! That doesn't seem very encouraging!
- Zenaps
    - Domains:
        - www.zenaps.com
    - Concerns:
        - Etsy is using Zenaps in order to drive my content engagement and boost sales

- Podsight
  - Domains:
    - Cdn.pdst.fm
  - Concerns:
    - Etsy is sharing my information in order to drive my listening to podcasts
- Akamai
  - Domains:
    - ocsp.godaddy.com.akadns.net
    - E8520.b.akamaiedge.net
  - Concerns:
    - Akamai is a giant content delivery network; they have a birds-eye-view of much of my traffic by virtue of being so large.
- The Trade Desk
  - Domains:
    - insight.adsrvr.org
    - js.adsrvr.org
    - Match.adsrvr.org
  - Concerns:
    - Etsy is sharing my information with TradeDesk in order to boost my engagement with ads.
- Let's Encyrpt
  - Domains:
    - R3.o.lencr.org
  - Concerns:
    - Let's Encrypt knows what webpages I am trying to validate.

(2) Now enable encrypted DNS in your browser (Links to an external site.) and repeat the above exercise.

- *Who can see that you've visited the website based on encrypted DNS queries?*
  - After flushing my local and browser caches, and requesting https://thisiswhyimbroke.com once again, I only observed my system making DNS queries to mozilla.cloudflare-dns.com.
  - Considering that this request is encrypted, my ISP no longer knows what domains I am requesting IP addresses for, but only that I am requesting IP addresses.
  - However, now I am putting a lot of trust in Cloudflare, as opposed to my ISP, as now they are the ones who know what sites I am requesting, by virtue of being solely responsible resolving my encrypted DNS requests.
- *Comment on the privacy tradeoffs with encrypted DNS. Some companies from part 1 can still see your browsing activity, and other companies might not be able to, yet some new companies may have now gained some visibility into your browsing.*
  - Cloudflare has gained a lot of insight into my browsing, while my ISP has lost most of theirs; moreover, I am now being protected from totally unauthorized observers snooping on, or spoofing responses to, my DNS traffic.

- However, this does not mitigate most of the concerns I raised in the previous section, since most of the companies tracking me through the use of websites like www.thisiswhyimbroke.com and www.etsy.com while using unsecure DNS can still do so after switching to DNS over HTTPS. These sites can still share information and try to violate my privacy by reconstructing my traffic and presence on the internet.