Unaccepted Third-Party Cookies as the/a Leading Indicator of CNAME Trackers

GIAC (GCIH) Gold Certification

Author: Dan Welygan, daninbusiness@gmail.com
Advisor: Sally Vandeven

Accepted: *August 1, 2021*

Abstract

CNAME-based trackers can allow advertisers to avoid cookie blocking restrictions and potentially introduce security risks. They are currently best detected via exploding and expanding all subdomain calls on a site and comparing against lists of known trackers. While that method works, it also impacts loading times. This research explores if the presence of third-party tracking cookies placed immediately on a user's browser without user consent are a helpful indicator that CNAME trackers are more likely in use, and if they offer a means to a more performant method of CNAME tracker blocking.

1. Introduction

1.1. Overview

Canonical Name records, more often referred to as CNAME records, are a cornerstone of internet infrastructure and allow one domain name to point to another (Mockapetris 1987). CNAME Cloaking is the practice of deliberately hiding a third-party tracker as a first-party tracker (Cointepas 2019). CNAME-cloaked trackers are becoming more common across the internet, and when used, can unintentionally cause leakage of sensitive data in first-party cookies (Dimova, et al. 2021). Due to the first-party nature inherent in CNAME cloaking, they naturally evade traditional third-party cookie or third-party tracker blocklists.

End users today can identify and block CNAME trackers through use of the uBlock Origin extension (Dao 2020), or through recent versions of the Brave Browser (Brave 2020). uBlock Origin attempts to pre-emptively resolve all URLs and links on a page to determine if any scripts, images, headers, or other parts of a given site are leveraging this approach to point to a known tracking, advertising, or even malicious domain or IP address (Abrams 2020).

1.2. Thesis

Given that the existing approach to identify “cloaked” CNAME trackers is somewhat resource intensive, perhaps other signals could suggest a greater likelihood of cloaked CNAME trackers in use.

The European Union’s General Data Protection Regulation (GDPR) (Wolford, 2019) requires that websites should not use advertising or tracking cookies without the express consent of the user (Koch 2019). In global practice, a significant number of sites still place cookies without consent (Trevisan, et al., 2019). Perhaps the websites that are not concerned about placing cookies without consent will also be more inclined to use CNAME tracking.

This research will attempt to answer if the presence of cookies placed without consent on a website are an indicator that the hosting website is more likely to be using cloaked CNAME tracking.

Dan Welygan, daninbusiness@gmail.com

1.3. Process Overview

The research method consisted of two parts: (1) analyzing a sample of websites to determine how many of those place cookies on the user's PC without consent, and (2) Of those sites, reviewing how many are using cloaked CNAME trackers.

The number of sites that overlap by having both cookies placed without consent and CNAME trackers should show a representative relationship regarding the presence of un-consented third-party cookies and the use of cloaked CNAME trackers.

1.4. Expected results

Consider the following aspects of the ever-evolving internet landscape: the expanding popularity of CNAME tracking (Dimova, et al. 2021), which is a response to the impending "cookie-pocalypse" brought about by continuing changes in browser behavior to mitigate third-party tracking (Newman, 2018). Further, it has been over three years since GDPR officially took effect, yet cookie placement without consent remains a challenge for the tech industry. However, regulatory enforcement is becoming clearer and building momentum (Lomas, 2021).

The combined forces of ongoing regulatory pressure and browser platform changes should be driving forward-thinking website owners to explore, refine, and expand their tracking tools to adapt to a world with much fewer third-party tracking cookies. Yet, sites still reliably earning revenue from third party cookies for advertising today are unlikely to stop using them if still profitable and enforcement is not imminent for a given owner.

There are websites that, despite GDPR, continue to place advertising and tracking cookies on devices without user consent (Trevisan, et al, 2019). Some of those site owners should be exploring the addition of CNAME tracking as another form of advertising to offset revenue lost as the browsing industry shifts to a model that increasingly blocks third-party cookies altogether (Hensel, 2020).

In the current moment where tracking technology, corresponding regulations, and enforcement continue to evolve and are in transition, the data should show some overlap and positive correlation of cases of sites using unconsented third-party tracking cookies and scripts and CNAME tracking.

2. The Environment

The following sections detail the background context and definitions on third-party cookies and CNAME trackers to be used with the later portions of this paper.

2.1. Third-party tracking and advertising cookies placed before consent

Cookies are small text files sent from a website that store data related to visits to that website.

Advertisers may use cookies to uniquely identify the user based on a wide range of characteristics, such as browsing behavior, hardware and software properties in use, or other identifiers.

One of the critical advantages of online advertising compared to offline media is the use of more customized tracking. Cookies offer another data point for advertisers to segment and distinguish their audience (Ramos, et al, 2008).

2.1.1. Third-Party vs. First-Party Cookies

First-party cookies are cookies issued by the same domain of the site visited. For example, a user goes to example.com, and cookies issued from example.com or any of its subdomains (such as mail.example.com) are considered first-party cookies. First-party cookies are generally used to support authentication, preferences, and other profiles that a given site owner deems necessary. While this information may be used for advertising purposes if the site owner chooses to share it, this is generally not what anti-advertising measures and laws aim to prevent.

Third-party cookies are cookies that are placed by another party while a user is visiting a given domain. For example, if a user goes to www.example.com and receives a cookie from Facebook.com, the Facebook cookie is considered a third-party cookie.

2.1.2. History

Initially, the web was designed and used as a communications medium among academics. As the adoption of the web grew across the world and beyond academia, advertising emerged as a method of collecting revenue for site hosts. Advertisers

invented ways to display ads and eventually refined their model to build profiles of demographic data and other user data to improve their advertising offerings.

Some of these improvements for the industry were achieved via leveraging existing web standards and technologies in ways well beyond their original intended use. Cookies are a showpiece example of this – essentially a small file in the browser where user preferences and choices are stored. The user does not need to manually reconfigure these settings on each visit to a particular website.

Through the pursuit of growth, advertisers found ways to build on these solutions and increase their usage to the point of obtrusiveness. Users also became less likely to respond to simple banners. The advertising industry developed more sophisticated, less visible methods of tracking user behavior, such as tracking pixels and scripts (Staff 2020).

The implementation of the GDPR was the first significant privacy regulation with a global reach that carried substantial financial penalties for violations. While the GDPR offers controls and regulations for various privacy rights, it requires user consent to use cookies for anything beyond basic site functionality. The GDPR is a European Union (EU) specific law. Still, as written, it applies to companies outside the EU and European Economic Area (EEA) that serve or track the data of EU/EEA residents. In such cases, the potential impact of the GDPR is global (European Commission 2016).

The GDPR and ePrivacy Directive (an EU law from 2009 that provides more detailed requirements on cookies) specify that users' consent is necessary before using any cookies, “except strictly necessary cookies” (Koch, 2019). The approach used in the analysis for this paper aims to focus on cookies placed without consent.

2.1.3. Significance of advertising cookies

Assuming that most websites with a global audience have an inherent financial incentive to avoid fines associated with GDPR violations, it would be expected that in 2021, most websites would avoid using any advertising cookies or trackers placed without user consent.

Based on survey data, users also do not like the idea of being tracked and having advertisers and other third parties build up an array of data on their online habits (regardless of if actual user behavior may be different) (Axier, et al., 2019). The pro-privacy sentiment of disliking tracking is likely contributing to the political success of pro-privacy regulation globally.

2.1.4. Challenges to identifying advertising cookies

Not all cookies and tracking scripts are created equal. In some cases, cookies may be placed on a user's device without consent for benign, "strictly necessary" reasons, such as load-balancing or automatically determining content and language to display based on IP address. The diversity of sources and links across the web makes unwanted cookie identification difficult on its own without an accurate, well-maintained blocklist.

Also, as mentioned earlier, while the GDPR is considered to have global reach as it applies to non-EU countries that target and sell to EU residents, there are undoubtedly many localized markets and services that do not target EU residents. These localized sites, outside of the EU, targeting and serving non-EU residents are not in scope for the GDPR, and are not obligated to modify their websites accordingly (European Commission 2016).

2.1.5. Current events in the industry

A discussion of cookies and tracking would not be complete without mentioning the attempts of Apple and Google to redefine how tracking works on the internet (Hense 2021). Apple has implemented default behaviors in its iOS and iPad Operating Systems that block and disable tracking by default. Google is proposing a new tracking standard that would replace third-party cookies, FLOC (Federated Learning of Cohorts), which aims to anonymously track and group web users into specific time-bound behavioral-based groups or "cohorts" that can respectively be targeted by advertisers (Bindra, 2021). While the long-term global impact of these measures remains to be seen at the time of writing, advertisers will likely be paying close attention to these developments. CNAME trackers represent a potential workaround for those advertisers wishing to continue their tracking efforts, as they appear to most browsers as first-party cookies, evading blocking countermeasures and allowing similar tracking capability.

2.2 CNAME Trackers

2.2.1 Definition

As noted in Section 1.1, CNAME Cloaking or CNAME Trackers are third-party tracking scripts or other advertising-related functions disguised as first-party trackers. This disguise protects them from third-party blocking since these tracking scripts appear as a first-party subdomain on a given website (Dimova, et al. 2021).

These trackers are sometimes interchangeably referred to as "Cloaked Trackers" or "Cloaked CNAME Trackers," but this paper will use "CNAME Trackers" as the standard term.

An example of non-tracking CNAME usage is how websites use subdomains for content management purposes. Since these are inherently part of a site, they are considered first-party:

subdomain.example.com resolves to example.com.

In practice, Google does this when loading fonts for its account login screen:
fonts.gstatic.com resolves to gstaticadssl.l.google.com

An example of CNAME Cloaking is when the subdomain points to a tracking site:

totallynothiding.example.com resolves to example.tracker.com

A real-world example is when Chase.com uses CNAME Cloaking to point to its Adobe tracking suite via the omtrdc.net domain (Adobe 2020):

target.chase.com resolves to jpmcbankna.tt.omtrdc.net

2.2.2 History

The use of CNAME references is foundational to the modern web (Mockapetris, 1987), though it has not traditionally been applied to harbor advertising and tracking scripts as a means of bypassing anti-advertising measures. As the usage of ad-blocking software increases, the application of CNAME-based cloaking for advertising and tracking purposes has proven to be an effective workaround to continue serving third-party cookies and trackers beyond blocklists (Gibson, 2021).

2.2.3 Importance of CNAME Trackers

CNAME trackers are a potential risk vehicle. In addition to potentially offering a way for tracking and surveillance measures to bypass blocking countermeasures, they can also obtain credentials and other sensitive data leaked from first-party cookies (Dimova, et al. 2021).

2.2.4 Challenges Identifying CNAME Trackers

CNAMEs are part of the fabric of the internet (Mockapetris, 1987), and leveraging third-party services for site optimization via CNAMEs is a common, benign use-case. Content delivery mechanisms, such as fast.ly, is one example. In the context of this widespread, non-malicious usage, the method of cloaking tracking scripts behind CNAME redirects may not immediately stand out among the legitimate traffic.

2.2.5 Current Events in the Advertising and Tracking Industry

CNAME tracking is gaining popularity, though still a relatively small percentage of overall activity on the web (Dimova, et al. 2021). The industry is anticipating changes, known as the "Cookie-pocalypse" (Hensel 2021). One adaption to this is CNAME tracking, and there is evidence that web tracking and advertising companies are already reaching out to web hosts in order to proactively adapt (Cointepas, 2019). Other research demonstrates increased CNAME tracker usage from 2019 to 2021 (Dimova et. al, 2021). This trend is expected to continue as third-party cookies and trackers will eventually be blocked by default in Chrome, although Google's current FLOC proposal (Bindra, 2021) is experiencing significant pushback from various browser vendors as it collects public feedback (Bohn, 2021). Google has recently extended its deadline to retire third-party cookies in Chrome in 2023 as it continues to iterate and refine its FLOC and Privacy Sandbox plans (Calburn 2021).

3. Research Methods

The research was conducted in a three-step process:

1. Testing for cookies placed without consent using a list of the top 10,000 URLs globally.

2. Testing the set of sites using cookies without consent on a browser with uBlock Origin installed to identify CNAME trackers.
3. Analysis of the resulting subset of sites that had both third-party cookies without consent and blocked known CNAME trackers.

3.1. The Source list

The 10,000 URLs used in the study were from a global list of the top 10 million websites. This is an open list to the public, based on Common Crawl, Common Search, and Open Page Rank Initiative (DomCop 2021). To ease recovery in potential timeout issues, the list of 10,000 URLs was divided into different sets of 1000 and ran in sequence.

3.2. The Python Script

The CookieCheck tool was ideal for identifying cookies placed without consent (Trevisan, et al. 2019. It provides a fresh Docker container for a 'headless' Google Chrome incognito browsing session for each site it visits, records the cookies and trackers that it receives, and attempts to distinguish between tracking cookies, tracking scripts, and other cookies. Given the nature of the tool, there's no actual user interactivity with the site, thus no consent can be given to cookie notices or banners if present. The fresh container and incognito mode also ensures there are no prior cookies or carryover from prior browsing that may influence what is recorded.

Modifying the tool allowed it to work through an input file containing many URLs rather than, as originally published, individual sites defined through line arguments. Details of the modifications used are in Appendix B.

3.2.1. Filtering the Results

The output from the script produced a list of each site visited and the associated tracking cookies, tracking scripts, and other cookies. Different sites have different combinations of cookies and scripts, if anything at all.

Excel was used for analysis purposes to filter out any results that did not contain anything in the "tracking cookies" category.

A user more proficient in scripting could likely build in some more automated processing to manage the Python output and perform some data filtering upfront to avoid working in Excel.

3.3. Testing for CNAME Trackers

Using some PowerShell scripting (see Appendix A) with portions of the list identified as URLs that placed third-party tracking cookies without consent, one could open multiple Private-Mode Firefox tabs (usually 50-100 at a time given performance constraints) to enable CNAME tracker inspection via the (previously installed) uBlock origin extension.

The Firefox version used at during research was version 88.0.1, on an Ubuntu 20.04.2 LTS 64-bit VM.

Filtering the uBlock Origin logger view to show only blocked CNAME trackers allowed an efficient, manual scan of sites to see which were serving CNAME trackers. The results where then noted, per site.

Once site review was complete, the data was consolidated in Excel to look at the overall trends.

4. Synthesis

Successfully completing the research required modification and adjustment of several tools.

4.1. Examination of the effectiveness of tools and results

The research was dependent on using several tools and methods together to obtain the needed results.

4.1.1. CookieCheck

During the research, the author forked the CookieCheck tool to work with a list of URLs and provide output in a way that allowed for easy analysis later. The modified script is in Appendix B.

Running this tool was most effective in sets of ~1000 URLs and would take ~2-4 hours to complete. This time length worked well and allowed for recovery in the event of a timeout that stopped the script. There was only one timeout experienced during testing over the three days spent running the script and gathering data.

4.1.2. Ghostery

The CookieCheck script itself is dependent on a tracker set listed as "ghostery_disconnect", which, based on the date of the last GitHub check-in, was current as of October 2017. A more current tracker list may influence the results in showing additional known domains used for advertising/tracking.

4.1.3. uBlock Origin and Firefox

The use of uBlock origin's functionality in Firefox to test and identify the presence of trackers is very manual. If one could reliably output the uBlock origin Logger results, then this could be scripted. Alternately, a user could also build functionality that duplicates uBlock's DNS resolver and integration with known ad-blocking lists.

This research used the default, "out of box" uBlock Origin blocklists, which include "EasyList", "EasyPrivacy", and "Peter Lowe's Ad and tracking server list."

4.1.4. Excel and data research

Excel was used for data analysis due to familiarity and comfort in using the tool to quickly transform data. It was well-suited for the task and dataset.

4.2. The list of sites investigated

There are various websites available that track and count variations of site popularity and page rank. Initial plans were to leverage a list from Alexa.com, though after subscribing, the lists were limited to 500 or 1000 sites each. The OpenPageRank

project appeared to be a viable alternative that was a good fit for the project given the global scope and measurement based on site activity (DomCop 2021).

4.3. Identifying CNAME Trackers

The results of this experiment are dependent upon the accuracy and validity of uBlock origin in Firefox's CNAME blocking list. Since the ad-tracking landscape continues to evolve and no blocking list can ever be 100% accurate, it's possible that some yet to be identified trackers were missed. An alternate approach would be to build a statistical heuristic (Dinova, et. al 2021), though building and implementing it was well beyond the scope of this research paper.

5. Findings and Discussion (Exposition of the Data)

Of the 10,000 websites analyzed from a dataset compiled from a US-based IP address from May 21-23, 2021, 3337 sites (nearly one-third) placed advertising or tracking cookies without user consent.

Thirty-nine sites (1.2% of 3,337) that placed advertising cookies before any explicit user consent also engaged in the use of CNAME trackers. This shows that the placement of third-party trackers without user consent remains fairly common in practice and is not a useful as a predictive indicator if CNAME trackers are in use.

Compared to the total population of 10,000 sites considered, this is an incidence of ~0.4%.

5.1. The CNAME Tracking Providers

Of the 39 sites that contained third-party cookies placed without consent and CNAME tracking, 17 (44%) were from Adobe, as shown by the overlap of a CNAME trackers that point to omtrdc.net and third-party cookies associated with demdex.net. Omtrdc and demdex are both Adobe-owned properties, as shown by the Adobe Experience Cloud privacy page at https://www.adobe.com/privacy/experience-cloud.html.

5.1.1. Adobe is also a third-party cookie Leader

Of the 10,000 sites reviewed, Adobe-related properties were present on 1130 of them. Comparing the presence of Adobe-based CNAME trackers relative to Adobe-based third-party cookies shows a 1.5% overlap, which is in line with the overall research results, which suggests that Adobe third-party cookies are no more likely to indicate CNAME tracking than the presence of any other third-party cookies.

5.1.2. Others

The second runner-up was Mailchimp, which had CNAME trackers in use on six out of the 39 sites.

After that, the remaining 16 sites had trackers spread among 11 other providers.

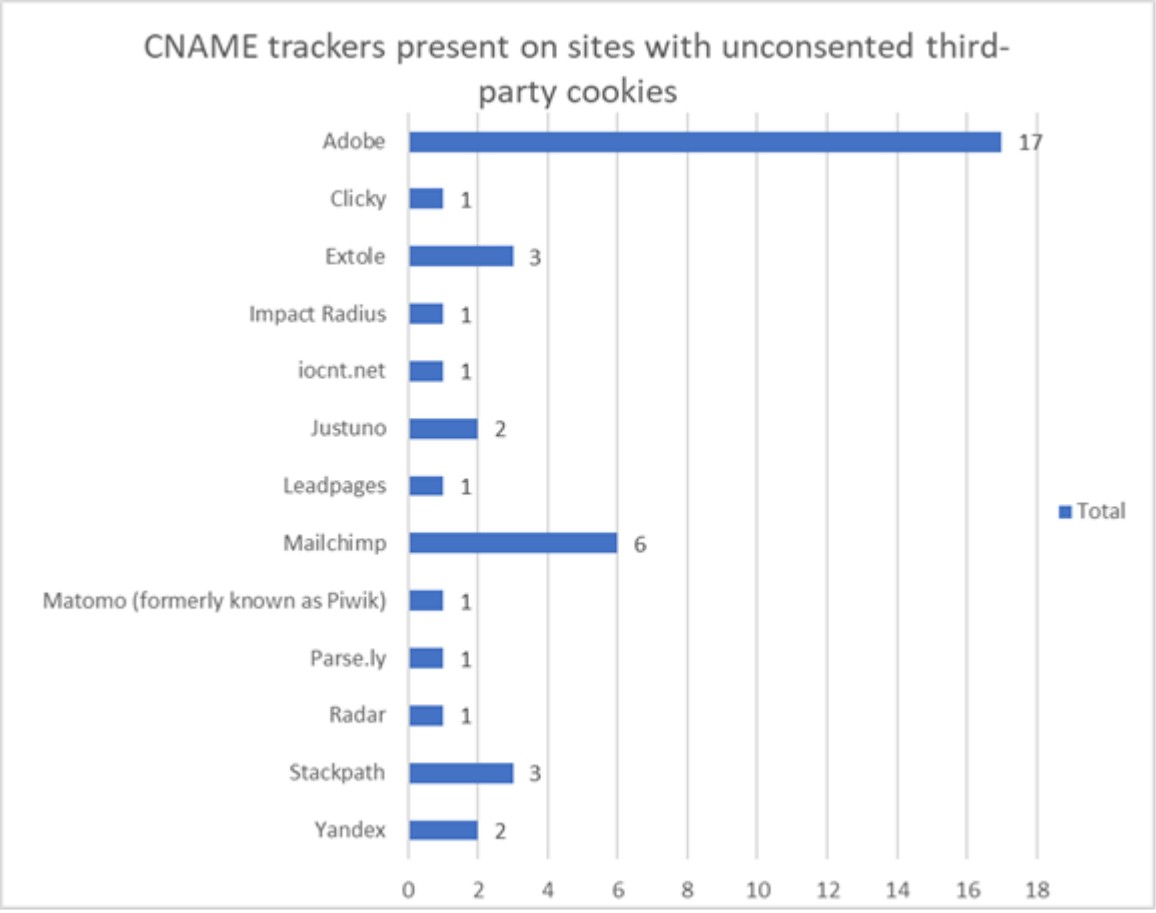

Figure 1. CNAME trackers present on sites with unconsented third-party cookies

5.1.3. The ratio of unconsented third-party cookies found in the dataset and CNAME Trackers

The results suggest that there are a handful of third-party cookies that are excellent indicators that a CNAME tracker is also present. Although the correlation was strong for this small group of cookies, the occurrence was rare, especially considering the 10,000 URL sample size.

The results also suggest that there are a few providers of CNAME trackers that either do not use third-party cookies at all or are (perhaps) using names for their cookies not obviously related to their business identity.

The table below shows the proportion of sites in the sample set that used third party cookies from a Tracking/Advertising Company and how that compares to the amount of CNAME trackers found.

Tracking/Advertising Company	Number of sites found with these companies' third-party cookies (out of 10,000 URL sample)	Number of sites found using these companies' Cname trackers in addition to unconsented third-party cookies	Proportion of an advertiser's CNAME trackers used with unconsented third-party cookies compared to the advertiser's third-party cookies identified in the 10,000 URL sample set
Adobe	1130	17	1.5%
Clicky	24	1	4.2%
Extole	0	3	N/A
Impact Radius	0	1	N/A
iocnt.net	0	1	N/A
Justuno	0	2	N/A
Leadpages	1	1	100.0%
Mailchimp	8	6	75.0%
Matomo (formerly known as Piwik)	0	1	N/A
Parse.ly	0	1	N/A
Radar	3	1	33.3%
Stackpath	2	2	100.0%
Yandex	135	2	1.5%

Table 1. Ratio of sites found using a tracking company's CNAME trackers vs the tracking company's total third-party advertising cookies in the sample set

5.1.4. Sites found to be using both unconsented third-party cookies and CNAME Trackers

This is the list of the 39 sites identified in the researched data set that had both unconsented third-party cookies and CNAME Trackers. A complete list including the CNAMEs and alias URLs is in Appendix C.

URL	CNAME Tracking Entity
http://slate.com	Parse.ly
http://mail.ru	Radar
http://aarp.org	Adobe
http://dell.com	Adobe
http://walgreens.com	Adobe
http://aaa.com	Adobe
http://gutandpsychologysyndrome.com	Justuno
http://thesilvers.leadpages.net	Leadpages
http://focus.de	iocnt.net
http://thefader.com	Mailchimp
http://musescore.com	Yandex
http://dangerousminds.net	Mailchimp
http://simonandschuster.com	Extole
http://webex.com	Adobe
http://mathworks.com	Adobe
http://chase.com	Adobe
http://bose.com	Adobe, Extole
http://cox.com	Adobe
http://draxe.com	Justuno
http://onextrapixel.com	Impact Radius
http://aircanada.com	Adobe
http://bloglines.com	Mailchimp
http://digitalmusicnews.com	Mailchimp
http://stonetemple.com	Stackpath
http://wegmans.com	Adobe
http://bitdefender.com	Adobe
http://books.simonandschuster.com	Extole
http://ultimate-guitar.com	Yandex

http://harley-davidson.com	Adobe
http://latrobe.edu.au	Adobe
http://abqjournal.com	Mailchimp
http://siriusxm.com	Adobe
http://nationwide.com	Adobe
http://casino.org	Clicky
http://jihadwatch.org	Stackpath
http://deakin.edu.au	Adobe
http://coolhunting.com	Mailchimp
http://architectureartdesigns.com	Stackpath
http://focusonthefamily.com	Matomo (formerly known as Piwik)

Table 2. Sites found that used both unconsented third-party cookies and CNAME Trackers

5.2. One CNAME tracking service per site, except…

Most of the sites identified that used CNAME trackers, were using CNAME trackers from only one tracking/advertising entity. However, Bose.com used CNAME trackers from two tracking/advertising entities, Adobe and Extole.

5.3. Other prominent Third-party trackers

The analysis results showed most third-party trackers do not have an inherently obvious domain name that correlates if a CNAME tracker is part of the same solution. Through a review of blocklists and web searching, one can (eventually) deduce the organization associated with the CNAME tracking effort.

Some of the big names in online advertising did, predictably, show as present among the data collected. Unless otherwise noted, none of them used CNAME trackers. Google (including Double-click), Facebook, and Amazon already have significant first-party user bases, products, and tracking mechanisms, therefore they do not have the urgency and need for exploiting CNAME tracking. Also, since Google, Facebook, and Amazon do provide services in the EU, intended for EU residents, they are clearly in scope for the GDPR and very likely have taken measures to comply. The lack of CNAME tracking data from these companies in the data reflects this.

Company	**Number of sites from the sample set of 10,000 that containing [company's] third-party trackers**
Adobe	1130
Amazon	1068
Facebook	2362
Google	647
Doubleclick	3546
Twitter	847
Yandex	135
Criteo	665

Table 3. Major third-party trackers identified in the 10,000 URL dataset

5.4. Unexpected Findings

As is often the case in research and experimentation, one may discover unanticipated results. The following sections describe these surprises in more detail.

5.4.1. Questionable uBlock Behavior

Of the 39 identified cases of CNAME tracking, there were six associated with the URL "d1zgderxoe1a.cloudfront.net". CloudFront is a content-delivery service offered by AWS (Amazon 2012).

Of these six cases, the usage all appears to be associated with the email service, Mailchimp. Also, while they are third-party trackers that leverage CNAME cloaking, the main URL does not appear to be a subdomain of the host site. Examples can be seen below:

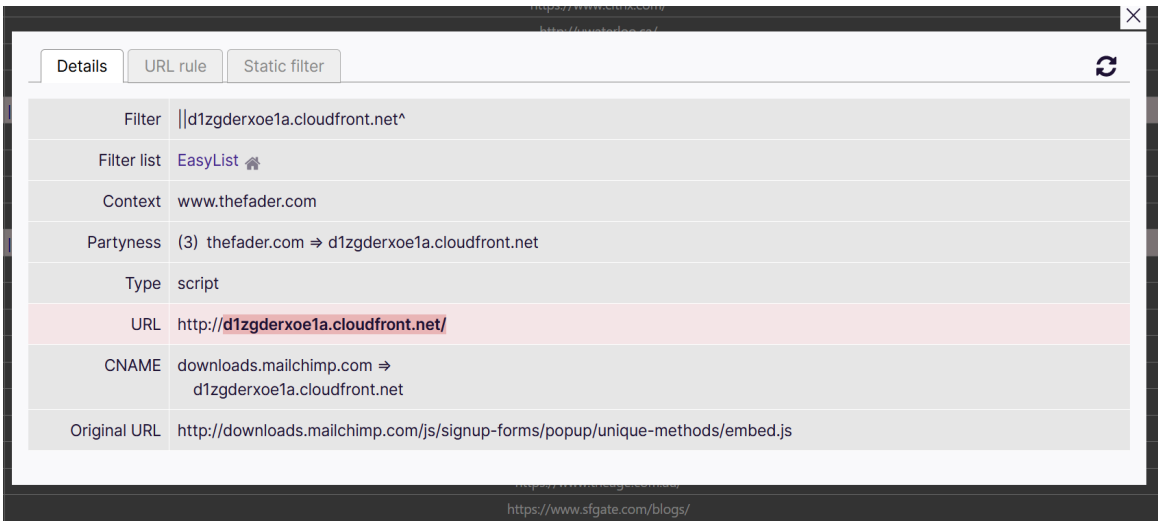

Figure 2. First example of Mailchimp flagged as CNAME tracker

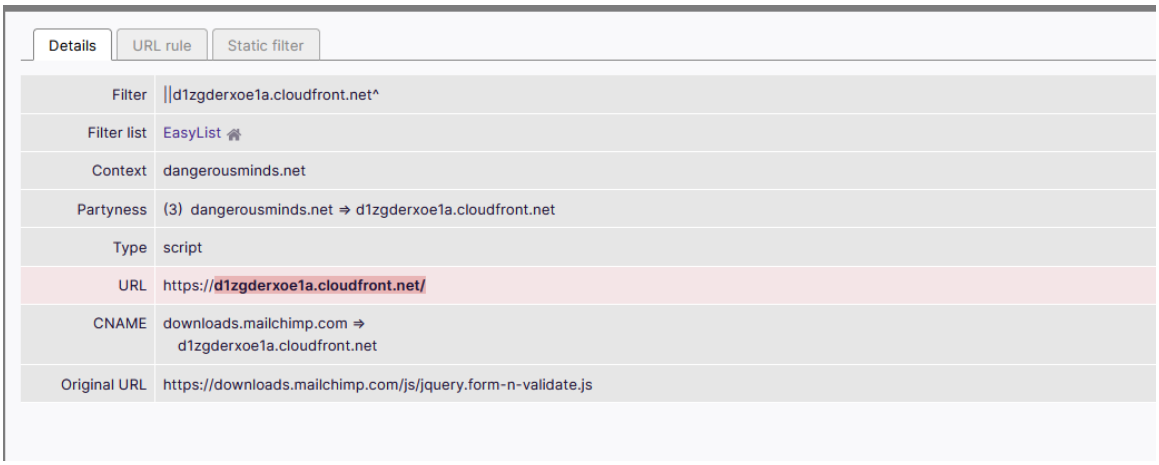

Figure 3. Second example of Mailchimp flagged as CNAME tracker

In contrast, the URL in this Omtrdc (Adobe) tracker is a subdomain of the host site.

Figure 4. Example of Omtrdc (Adobe) CNAME tracker

If one expects uBlock Origin to identify all cases of CNAME cloaking on a given site, then this behavior is working as intended. On the other hand, the examples with d1zgderxoe1a.cloudfront.net appear to have no correlation to a first-party subdomain on the host site; they appear more as instances of CNAME links used with what is already obviously a third-party, as is commonly seen with content delivery networks such as fast.ly.

Similar yet distinct in its own way, the site http://thesilvers.leadpages.net was flagged as using CNAME tracking, although what was shown as the "cloaked" URL turned out to be another subdomain of leadpages.net. Leadpages.net appears to be a webhosting and commerce platform for small businesses (Leadpages 2021). This implementation of CNAME tracking may be how Leadpages offers some packaged analytics for customers.

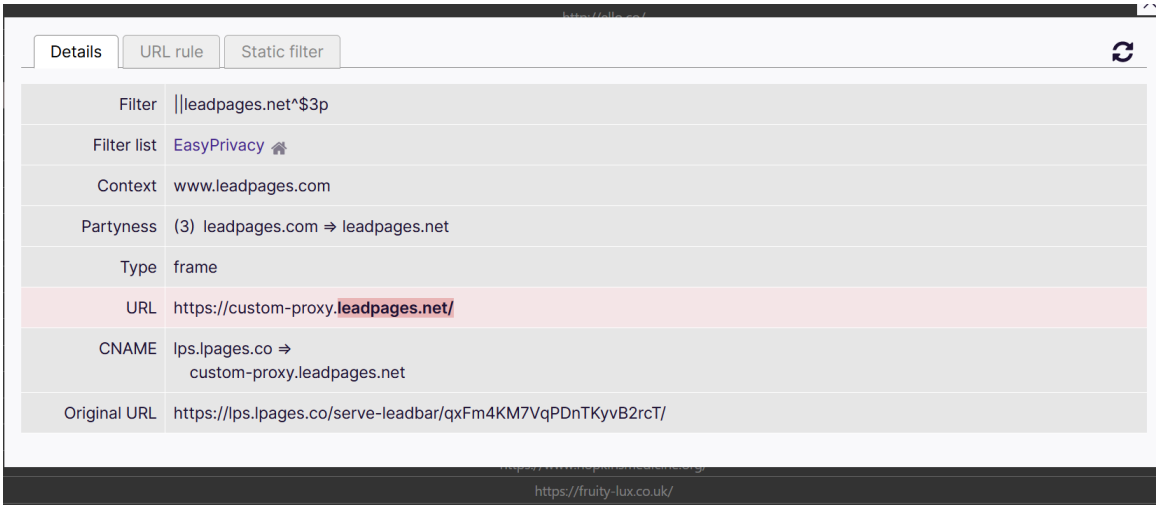

Figure 5. Example of Leadpages flagged as CNAME tracker

5.4.2. Firefox blocking/unblocking

In the space between the original proof of concept work for this paper in April 2021 and the actual bulk data collection performed in May 2021, Firefox appears to have taken a more aggressive stance against accessing specific sites. For example, www.ultimate-guitar.com was among the 39 websites identified that used both unconsented third-party advertising cookies and CNAME trackers. While Firefox blocked access to this site while collecting data, on further review, in June 2021, this site is now accessible again.

5.4.3. Lack of Criteo in the CNAME tracking results

Criteo, one of the sites shown in other CNAME research (Dimova et al, 2021) and referenced in other sources concerning CNAME tracking, was not represented among any of the identified CNAME trackers. Criteo third-party trackers were present on 665 of the total 10,000 sites used in this study, and 112 sites that placed cookies without consent contained Criteo trackers.

6. Recommendations and Implications for Future Research

This research shows that at current rates, ~1-2% of a population of websites that place cookies without consent would also use some CNAME tracker. Considering the rapid pace of change in the industry, it seems likely that if one were to repeat this same experiment several times over a year, one would see a growing trend emerge.

Additionally, variations in tooling and other options could likely produce additional insights.

6.1. Recommendations for Practice

Future researchers on this topic could:

- Double-check the efficacy and currency of the CNAME tracker blocklist they are using; this space appears to be developing in fits and starts.
- Explore ways to automate the output and review of the uBlock Origin Logger.
- Closely monitor developments with the third-party tracking cookie "cookie-pocalypse", as enforcement from browser vendors draws nearer, it is likely that more website owners will apply different strategies, including CNAME trackers.
- Closely monitor known entities that sell CNAME solutions and what their cookie aliases are.
- If continuing to use the CookieCheck script, definitely leverage the updates listed in Appendix B (or something similar) to process many sites at a time.

6.2. Implications for Future Research

There are many potential variations one could explore on this research, time and skill permitting:

- When reviewing sites known to place third-party cookies without consent, compare if there is a reduction in the third-party cookies placed if the user does not consent, and see if that impacts the CNAME trackers found.
- Check if specific sites that are geo-optimizing would have different tracker behavior. For example, if the user was shown as a user based in Turkey rather than the US.
- Explore variations in trackers used and detected while using different browsers on different platforms; Safari on iOS and macOS as well as Brave might show some differences.
- If possible, obtain and note the proportion of iPhone users on the sites where CNAME usage is up.
- Track the variation of CNAME tracker usage over time in general; one expects to see continued growth as cookiepocalypse comes closer.
- Explore the impact in triggering CNAME trackers from doing more in-depth interaction with a site, such as visiting sub-pages, registering users, etc.
- Track presence of CNAME trackers relative to site/host geography. Are they more likely in locations and geographies with more restrictive privacy laws?
- Perform a more detailed analysis on the trackers Radar, Mailchimp, Justuno, and Extole. Why is the frequency of CNAME tracker usage high relative to their -third-party cookie usage?
- Understand why uBlock shows Leadpages as a CNAME tracker; is there a way to refine the blocking behavior? Is that desirable?
- Slice and compare the use of Unconsented third-party cookies + CNAME tracking vs. Tracking Scripts + CNAME tracking. This paper focused on the former.
- Try applying some of the competing CNAME blocker lists for comparison of efficacy.
- Does Mailchimp do tracking in the situations uBlock Origin flags as CNAME tracker? Or is there some quirk in uBlock's logic?

7. Conclusion

As of the sample set investigated in May and June 2021, there is a 1.2% relationship between third-party tracking cookies placed without consent and the presence of actual CNAME trackers. While this relationship is not strong enough to be a helpful predictive indicator for general-purpose CNAME tracker blocking applications, it may at least show some basis for the frequency of CNAME trackers detected in the wild.

CNAME trackers are likely to remain a tool in the advertiser's toolbox that merits continued monitoring due to the potential privacy and security implications. Using the presence of third-party tracking cookies as a proxy to accelerate or prioritize CNAME analysis on a given site does not appear to offer significant time-saving benefits or efficiencies at this time.

References

Dimova, Acar, Olejnik, Joosen, Van Goethem. (2021, March 5). *The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion*. arXiv.org e-Print archive. https://arxiv.org/pdf/2102.09301.pdf

Trevisan, Traverso, Bassi, and Mellia. (2019, April). *4 years of EU cookie law: Results and lessons learned*. CORE – Aggregating the world's open access research papers. https://core.ac.uk/display/234925971?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1

DomCop. (2021). *Top 10 million websites based on Open data from Common Crawl & Common Search*. DomCop. https://www.domcop.com/top-10-million-websites.

DomCop. (2021, June 3). What is Open PageRank? https://www.domcop.com/openpagerank/what-is-openpagerank.

GitHub (2021) gorhill/uBlock. https://github.com/gorhill/uBlock/wiki/The-logger

Newman, L. H. (2018, June 4). *WWDC 2018: Apple Just Made Safari the Good Privacy Browser*. Wired. https://www.wired.com/story/apple-safari-privacy-wwdc/.

Hensel, A. (2020, January 21). *Cookiepocalypse: What the death of the third-party cookie means for retailers*. Modern Retail. https://www.modernretail.co/platforms/cookiepocalypse-what-the-death-of-the-third-party-cookie-means-for-retailers/.

Lomas, N. (2021, May 31). *Europe's cookie consent reckoning is coming*. TechCrunch. https://techcrunch.com/2021/05/30/europes-cookie-consent-reckoning-is-coming/.

Gibson, S. (2021, March 2). *CNAME Collusion*. GRC.com. https://www.grc.com/sn/sn-808.pdf.

Mockapetris, P. (1987, November). RFC 1035 - Domain Names - Implementation and Specification. https://datatracker.ietf.org/doc/html/rfc1035#section-3.2.2.

Cointepas, R. (2019, December 18). *CNAME Cloaking, the dangerous disguise of third-party trackers*. Medium. https://medium.com/nextdns/cname-cloaking-the-dangerous-disguise-of-third-party-trackers-195205dc522a.

Bindra, C. (2021, January 25). *Building a privacy-first future for web advertising*. Google. https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/.

Bohn, D. (2021, April 16). *Nobody is flying to join Google's FLoC*. The Verge. https://www.theverge.com/2021/4/16/22387492/google-floc-ad-tech-privacy-browsers-brave-vivaldi-edge-mozilla-chrome-safari.

Ramos, Andreas; Cota, Stephanie (14 September 2008). Search Engine Marketing. *Google's Role in the Digitization of Analog Media - First Para. p. 5-6.* ISBN 9780071597340.

Koch, R. (2019, May 9). *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.eu. https://gdpr.eu/cookies/.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, August 17). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Amazon. *Amazon Cloudfront*. Amazon. https://aws.amazon.com/cloudfront/. Accessed 2021, June 19.

Wolford, B. (2019, February 13). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/.

Gazvoda, U. (2021). *Free, open-source ad content blocker.* uBlock Origin. https://ublockorigin.com/.

Abrams, L. (2020, February 25). *uBlock Origin 1.25 Now Blocks Cloaked First-Party Scripts, Firefox Only*. BleepingComputer. https://www.bleepingcomputer.com/news/security/ublock-origin-125-now-blocks-cloaked-first-party-scripts-firefox-only/.

Matte, C., Bielova, N., & Santos, C. (2020, February 21). *Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework*. arXiv.org. https://arxiv.org/abs/1911.09964.

CookieChecker. (2017). *CookieChecker/CookieCheckSourceCode*. GitHub. https://github.com/CookieChecker/CookieCheckSourceCode.

Ren, T., Wittman, A., De Carli, L., Davidson, D., (2021, February 25). "An Analysis of First-Party Cookie Exfiltration due to CNAME Redirections". https://web.cs.wpi.edu/~ldecarli/docs/papers/madweb21-cloaking.pdf

Dao, H. (2020, August 4). Characterizing CNAME cloaking-based tracking. https://blog.apnic.net/2020/08/04/characterizing-cname-cloaking-based-tracking/.

Toth, M., Bielova, N., Santos, C., Roca, V., Matte, C., "Contribution to the public consultation on the CNIL's draft recommendation on "cookies and other trackers"". 2020. ffhal-0249053. https://hal.inria.fr/hal-02490531/document.

Squarcina, M., Tempesta, M., Veronese, L., Calzavara, S., Maffei, M., "Can I Take Your Subdomain? Exploring Related-Domain Attacks in the Modern Web". 2020. https://arxiv.org/pdf/2012.01946.pdf.

Adobe. (2020, July 28). Adobe Experience Cloud privacy. https://www.adobe.com/privacy/experience-cloud.html.

Dan Welygan, daninbusiness@gmail.com

Stefanie Olsen (January 2, 2002). "Nearly undetectable tracking device raises concern". CNET News. Retrieved July 11, 2021.

Staff, V. (2019, July 3). *What is a tracking pixel and can strangers really spy on me through email?* The Verge. https://www.theverge.com/2019/7/3/20681508/tracking-pixel-email-spying-superhuman-web-beacon-open-tracking-read-receipts-location.

European Commission. (2016, August 30). *Art. 3 GDPR – Territorial scope*. General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-3-gdpr/.

Claburn, T. (2021, June 24). *Google: About that whole getting rid of third-party cookies thing – we're gonna need another year or so*. The Register® - Biting the hand that feeds IT. https://www.theregister.com/2021/06/25/google_thirdparty_cookies/.

Leadpages. (2021). *Website & Landing Page Software Small Businesses*. Leadpages. https://www.leadpages.com/.

Brave. (2020, November 2). *What's brave done for my Privacy Lately? EPISODE #6: Fighting CNAME TRICKERY*. Brave Browser. https://brave.com/privacy-updates-6/.

Appendix A

PowerShell

The following PowerShell script below aided in opening multiple sites within a Firefox private browsing window.

```
$urls = @("https://google.com/","https://www.youtube.com/","https://www.facebook.com")
foreach($url in $urls){
start "C:\Program Files\Mozilla Firefox\firefox.exe" -ArgumentList @( '-private-window' , $url)
   Start-Sleep -Seconds 1
}
```

Appendix B

Python Changes

Originally, the Python script used with the CookieCheck tool, as provided on the Github site (https://github.com/CookieChecker/CookieCheckSourceCode), required a command-line argument per URL. The modifications made, shown below, allow the script to work from a file containing a list of URLs and provide output in the format that specifies the URL visited in addition to the cookies found.

This updated script is available here:
https://github.com/DangDan987/CookieCheckSourceCode

Output was collected by using the Linux command-line convention to output to a file.

For example, to execute in a Linux environment:

python3 testsite.py > output_DATE.txt

```
#!/usr/bin/python3

import PyChromeDevTools
import time
import sys
import subprocess
import os
import json
import signal
import shutil
import random
import re
import fileinput #this was a new thing I added

PORT=random.randint(2000,10000)
PROFILE_DIR="/tmp/tester_profile_" +str(PORT)
CHROME_CMD="google-chrome --remote-debugging-port="+str(PORT)+" --headless --user-data-dir="+PROFILE_DIR
MIN_TIME = 60*60*24*30 # 1 MONTH
tracker_file="trackers_ghostery_disconnect"
filepath = "specifyyourinputfilehere" #point to the flat file with a list of URLs you are using for input
```

```
SHORT_TIMEOUT=1
LONG_TIMEOUT=60

# Global vars
tracker_list=set()

def main():
    for line in fileinput.input(files=(filepath)): #this is how I get the loop started
        # Parse Arg
        # Strip Eventual "http://"
        if "/" in line:
            url = line
        else:
            url="http://" + line + "/"

        # Load Tracker List
        global tracker_list
        with open(tracker_file, 'r') as f:
            for line in f:
                tracker_list.add(line.strip())

        # Start Chrome
        shutil.rmtree(PROFILE_DIR, ignore_errors=True)
        FNULL = open(os.devnull, 'w')
        proc = subprocess.Popen(CHROME_CMD, shell=True, stdin=None, stdout=FNULL,
                                stderr=subprocess.STDOUT, close_fds=True, preexec_fn=os.setsid)
        time.sleep(SHORT_TIMEOUT)

        # Connect Python wrapper
        chrome = PyChromeDevTools.ChromeInterface(port=PORT)
        chrome.Network.enable()
        chrome.Page.enable()

        # Navigate to URL and wait it to load
        start_time=time.time()
        chrome.Page.navigate(url=url)
        _,messages_1=chrome.wait_event("Page.frameStoppedLoading", timeout=LONG_TIMEOUT)
        time.sleep(SHORT_TIMEOUT*2)
        messages_2=chrome.pop_messages()

        chrome.Page.navigate(url=url)
        _,messages_3=chrome.wait_event("Page.frameStoppedLoading", timeout=LONG_TIMEOUT)
```

```
time.sleep(SHORT_TIMEOUT*2)
messages_4=chrome.pop_messages()

# Get all contacted domains
all_domains=set()
messages=messages_1+messages_2+messages_3+messages_4
for m in messages:
    if "method" in m and m["method"] == "Network.responseReceived":
        try:
            this_domain=m["params"]["response"]["url"].split("/")[2]
            all_domains.add(this_domain)
        except:
            continue

# Find Cookies and Trackers
first_party=get2LD(url.split("/")[2])
result={"trackers_cookies":set(),"trackers_no_cookies":set(), "other_cookies":set()}
cookies=chrome.Network.getAllCookies()
for cookie in cookies["result"]["cookies"]:
    if is_tracker(cookie["domain"]):
        tracker=True
    else:
        tracker=False

    if get2LD(cookie["domain"]) != first_party:
        third_party=True
    else:
        third_party=False

    if cookie["expires"] - start_time > MIN_TIME:
        persistent=True
    else:
        persistent=False

    if tracker and persistent:
        result["trackers_cookies"].add(cookie["domain"].strip("."))
    elif third_party and not tracker and persistent:
        result["other_cookies"].add(cookie["domain"].strip("."))

# Add trackers without cookie
for domain in all_domains:
    try:
```

```
            domain_SLD=getGood2LD(domain)
            if is_tracker(domain):
               if not domain     in result["trackers_cookies"] and \
                  not domain_SLD in result["trackers_cookies"] and \
                  not domain     in result["other_cookies"]    and \
                  not domain_SLD in result["other_cookies"]:
                   result["trackers_no_cookies"].add(domain)
         except:
            continue
      # Convert sets to lists
      for k in result:
         result[k]=list(result[k])
      print (url, json.dumps(result)) #this includes the url per set of cookies

      # Kill Chrome and delete profile
      os.killpg(os.getpgid(proc.pid), signal.SIGTERM)
      shutil.rmtree(PROFILE_DIR, ignore_errors=True)


def is_tracker(host):

   global tracker_list

   if host             in tracker_list or \
      getGood2LD(host) in tracker_list or \
      get3LD (host)    in tracker_list:
       return True

   else:
      return False


# False TLDs
bad_domains=set("co.uk co.jp co.hu co.il com.au co.ve .co.in com.ec com.pk co.th co.nz com.br com.sg com.sa \
com.do co.za com.hk com.mx com.ly com.ua com.eg com.pe com.tr co.kr com.ng com.pe com.pk co.th \
com.au com.ph com.my com.tw com.ec com.kw co.in co.id com.com com.vn com.bd com.ar \
com.co com.vn org.uk net.gr".split())

# Cut a domain after 2 levels
# e.g. www.google.it -> google.it
def get2LD(fqdn):
   if fqdn[-1] == ".":
```

```
        fqdn = fqdn[:-1]
    names = fqdn.split(".")
    tln_array = names[-2:]
    tln = ""
    for s in tln_array:
        tln = tln + "." + s
    return tln[1:]

# Cut a domain after 2 levels considering long TLDs
# e.g. www.google.it -> google.it
def getGood2LD(fqdn):
    if fqdn[-1] == ".":
        fqdn = fqdn[:-1]
    names = fqdn.split(".")
    if ".".join(names[-2:]) in bad_domains:
        return get3LD(fqdn)
    tln_array = names[-2:]
    tln = ""
    for s in tln_array:
        tln = tln + "." + s
    return tln[1:]

# Cut a domain after 3 levels
# e.g. www.c3.google.it -> c3.google.it
def get3LD(fqdn):
    if fqdn[-1] == ".":
        fqdn = fqdn[:-1]
    names = fqdn.split(".")
    tln_array = names[-3:]
    tln = ""
    for s in tln_array:
        tln = tln + "." + s
    return tln[1:]

main()
```

Appendix C

Sites found using unconsented third-party and CNAME trackers, including alias and actual tracking URLs

URL	CNAME Tracking Entity	Alias (first party) URL	Actual Tracking URL
http://slate.com	Parse.ly	https://fpa-cdn.slate.com/keys/slate.com/p.js	https://fpa-cdn-slate-com.parsely.com/
http://mail.ru	Radar	https://xray.mail.ru/batch?p=whiteline&pgid=kp0kx3xh.cu	https://common.radar.imgsmail.ru/
http://aarp.org	Adobe	https://sjourney.aarp.org/m2/aarp/mbox/json?mbox=target-global-mbox-aarp&mboxSession=1bd7fd867780476093d8dc2ca410e5b3&mboxPC=&mboxPage=9f4d49b6b1c2454996d07ef353c7335e&mboxRid=ee456d8c963545eea667926960002efe&mboxVersion=1.8.2&mboxCount=1&mboxTime=1621798333024&mboxHost=www.aarp.org&mboxURL=https%3A%2F%2Fwww.aarp.org%2F&mboxReferrer=&mboxXDomain=enabled&browserHeight=1058&browserWidth=1903&browserTimeOffset=-420&screenHeight=1200&screenWidth=1920&colorDepth=24&devicePixelRatio=1&screenOrientation=landscape&webGLRenderer=ANGLE%20(NVIDIA%20GeForce%20GTX%201070%20Direct3D11%20vs_5_0%20ps_5_0)&tags=taxonomy%3Aaarp&title=AARP%C2%AE%20Official%20Site%20-%20Join%20%26%20Explore%20the%20Benefits&level0=aarp&keywords=aarp%2C%20real%20possibilities%2C%20baby%20boomers%2C%20driver%20safety%2C%20over%2050%2C%20medicaid%2C%20medicare%2C%20online%20games%2C%20travel%20deals%2C%20caregiv	https://aarp.tt.omtrdc.net/

		ers%2C%20election%20news%2C%20retirement%20calculator%2C%20retirement%20plan%2C%20social%20security%2C%20online%20community%20&tagTitles=aarp&at_property=fb36a4ed-86e4-0d0d-2ffc-75c6b996f792&affinityCategory=false&mboxMCSDID=6E12BFEAD916264E-36FAB7BA60AD7CE6&mboxMCGVID=68168282592573791001200046147928504314 https://stt.dell.com/m2/dellinc/mbox/json?mbox=dell-global-mbox&mboxSession=75d42afaf54d4f0eb86d6ba892cf1471&mboxPC=&mboxPage=b1fe94440e464d60be909c0d41376627&mboxRid=9a01f13ab7924b0a9b50ca00a9e9894f&mboxVersion=1.8.0&mboxCount=1&mboxTime=1621799256344&mboxHost=www.dell.com&mboxURL=https%3A%2F%2Fwww.dell.com%2Fen-us&mboxReferrer=&mboxXDomain=enabled&browserHeight=1058&browserWidth=1903&browserTimeOffset=-420&screenHeight=1200&screenWidth=1920&colorDepth=24&devicePixelRatio=1&screenOrientation=landscape&webGLRenderer=ANGLE%20(NVIDIA%20GeForce%20GTX%201070%20Direct3D11%20vs_5_0%20ps_5_0)&pgCMS=csb_homepage&pgCountry=us&pgCustomerset=uscorp1&pgLanguage=en&pgSegment=gen&pgname=dell.com%20responsive%20homepage&viewport=&productid=&authState=&at_property=b7ae968b-52b6-dfde-d9f3-ae9d30ce6f99&profile.crmdata=empty&timeout=2000&mboxMCSDID=51945CAC459650D0-38332AA53E611EA6&vst.trk=nsm.dell.com&vst.trks=sm.dell.com&mbo	
http://dell.com	Adobe		https://dellinc.tt.omtrdc.net/

http://walgreens.com	Adobe	xMCGVID=45463195486388718856320580001924727897 https://target.walgreens.com/rest/v1/delivery?client=walgreenco&sessionId=2cca3e38d83e4326a5be05019d42d601&version=2.3.3	https://walgreenco.tt.omtrdc.net/
http://aaa.com	Adobe	https://mcdmetrics2.aaa.com/m2/aaanortheast/mbox/json?mbox=ne-nav-promo-news-safety&mboxSession=a2de56db77964099aa2023b61f96cbf8&mboxPC=&mboxPage=3126b00b26d64444be68055b06f11cb8&mboxRid=022fac11aa19497b9db27e6137afc1a0&mboxVersion=1.8.2&mboxCount=7&mboxTime=1621962174961&mboxHost=wa.aaa.com&mboxURL=https%3A%2F%2Fwa.aaa.com%2F%3Fzip%3D98422%26stateprov%3Dwa%26city%3Dtacoma%26devicecd%3DTB&mboxReferrer=&mboxXDomain=enabled&browserHeight=801&browserWidth=1230&browserTimeOffset=-420&screenHeight=1003&screenWidth=1504&colorDepth=24&devicePixelRatio=1.5&screenOrientation=landscape&webGLRenderer=ANGLE%20(Intel(R)%20Iris(R)%20Plus%20Graphics%20Direct3D11%20vs_5_0%20ps_5_0)&mboxMCSDID=5DB5C708CAEF5559-71B3D7439E26EEE2&vst.trk=mcdmetric.aaa.com&vst.trks=mcdmetrics.aaa.com&mboxMCGVID=61303674790267326685642190043396985192	https://aaanortheast.tt.omtrdc.net/
http://gutandpsychologysyndrome.com	Justuno	https://scripttags.jst.ai/shopify_justuno_36437753994_25de1720-edef-11ea-aee1-9d341c2767db.js?shop=getsmidge.myshopify.com	https://scripttags.justuno.com/
http://thesilvers.leadpages.net	Leadpages	https://lps.lpages.co/serve-leadbar/qxFm4KM7VqPDnTKyvB2rcT/	https://custom-proxy.leadpages.net/

http://focus.de	iocnt.net	https://data-1818d50639.focus.de/sensor.modern.ncl.min.js	https://relay-client-c01.iocnt.net/
http://thefader.com	Mailchimp	http://downloads.mailchimp.com/js/signup-forms/popup/unique-methods/embed.js	http://d1zgderxoe1a.cloudfront.net/
http://musescore.com	Yandex	https://mc.yandex.com/watch/46196364?wmode=7&page-url=https%3A%2F%2Fmusescore.com%2F&charset=utf-8&browser-info=pv%3A1%3Agdpr%3A14%3Avf%3Abx1nzewshzamry6%3Afu%3A0%3Aen%3Autf-8%3Ala%3Aen-US%3Av%3A530%3Acn%3A1%3Adp%3A0%3Als%3A392401626797%3Ahid%3A460158687%3Az%3A-420%3Ai%3A20210527222355%3Aet%3A1622179435%3Ac%3A1%3Arn%3A507573116%3Arqn%3A1%3Au%3A16221794353217357 33%3Aw%3A1230x801%3As%3A1504x1003x24%3Ask%3A1.5%3Ans%3A1622179433609%3Ads%3A2%2C69%2C394%2C158%2C564%2C0%2C%2C60%2C%2C%2C%2C%2C%2C%3Adsn%3A1%2C69%2C395%2C0%2C565%2C571%2C%2C174%2C%2C%2C%2C%2C%3Arqnl%3A1%3Aadb%3A1%3Afip%3Afb1001b28495989221a2a965042f9e3c-a81f3b9bcdd80a361c14af38dc09b309-a81f3b9bcdd80a361c14af38dc09b309-08cddc828a0a4cecdead9052886a5778-6456f00690ac9fc94dca4eb4fd6d061a-9b01b6a68dffdd86560f187ebe2649ec-61b9878bbce18de73aafc8582a198c0c-65112a363b745b2811c7267d45779933-a81f3b9bcdd80a361c14af38dc09b309-c6d7b47b2dcff33f80cab17f3a360d0	https://mc.yandex.ru/

		b-8f94aaac7063d09db7443126fff264fc%3Ati%3A2%3Ast%3A1622179437%3At%3AFree%20sheet%20music%20sorted%20by%20view%20count%20%7C%20Musescore.com	
http://dangerousminds.net	Mailchimp	https://downloads.mailchimp.com/js/jquery.form-n-validate.js	https://d1zgderxoe1a.cloudfront.net/
http://simonandschuster.com	Extole	https://share.simonandschuster.com/core.js	https://simon-and-schuster.extole.io
http://webex.com	Adobe	https://tmetrics.webex.com/rest/v1/delivery?client=ciscosystemsinc&sessionId=6057cd03349b4dd48b898aaa42d20fed&version=2.4.0	https://ciscosystemsin.tt.omtrdc.net/
http://mathworks.com	Adobe	https://starget.mathworks.com/rest/v1/delivery?client=themathworksinc&sessionId=c383957b751c489ab5e5df059e90b377&version=2.4.1	https://themathworksinc.tt.omtrdc.net/
http://chase.com	Adobe	https://target.chase.com/rest/v1/delivery?client=jpmcbankna&sessionId=ab7b1eeb0f8b4d4587e1aafca6f66b21&version=2.3.2	https://jpmcbankna.tt.omtrdc.net/
http://bose.com	Adobe, Extole	https://target.bose.com/rest/v1/delivery?client=bose&sessionId=4ae95ec2e0ed4c268eda57207f71c1b6&version=2.3.1 https://refer.bose.com/core.js	https://cnamecustomer.tt.omtrdc.net/ https://bose.extole.io/
http://cox.com	Adobe	https://target.cox.com/rest/v1/delivery?client=coxcommunications&sessionId=b9e5a8de61cf474f8644b6e051394c19&version=2.2.0	https://coxcommunications.tt.omtrdc.net/
http://draxe.com	Justuno	https://cdn.jst.ai/vck-wp.js	https://cdn.justuno.com/
http://onextrapixel.com	Radius	https://1.envato.market/i/37019/350699/4662	https://1-envato-market.ct.impactradius.com/
http://aircanada.com	Adobe	https://starget.aircanada.com/m2/aircanada/mbox/json?mbox=target-global-mbox&mboxSession=79805988ae4c4b5ca1bf0c030f7620ad&mboxPC=&mboxPage=b61362e82f43482ebe31162003dbfa82&mboxRid=8b0695008ff340c791233bfde72742fc&mboxVersion=1.8.1&mboxCount=1&m	https://aircanada.tt.omtrdc.net/

boxTime=1622226970178&mboxHost=www.aircanada.com&mboxURL=https%3A%2F%2Fwww.aircanada.com%2Fus%2Fen%2Faco%2Fhome.html&mboxReferrer=&mboxXDomain=enabled&browserHeight=801&browserWidth=1230&browserTimeOffset=-420&screenHeight=1003&screenWidth=1504&colorDepth=24&devicePixelRatio=1.5&screenOrientation=landscape&webGLRenderer=ANGLE%20(Intel(R)%20Iris(R)%20Plus%20Graphics%20Direct3D11%20vs_5_0%20ps_5_0)&siteInfo.webProperty=aircanada.com&siteInfo.name=Global%20Site&siteInfo.type=Responsive&siteInfo.environment=AEM&siteInfo.viewportSize=large&siteInfo.appVersion=&siteInfo.buildDate=2021-05-28&siteInfo.screenWidth=1230&siteInfo.screenHeight=801&siteInfo.siteEdition=us&siteInfo.language=en&pageInfo.pageName=aco%7Chome&pageInfo.pageTitle=Air%20Canada%20-%20The%20Official%20Website&pageInfo.url=https%3A%2F%2Fwww.aircanada.com%2Fus%2Fen%2Faco%2Fhome.html&pageInfo.previousPageName=&pageInfo.previousPageURL=&pageInfo.pageHierarchy.level1=aco&pageInfo.pageHierarchy.level2=home&pageInfo.pageType=home&pageInfo.previousPageLinkName=&pageInfo.accessibility=true&pageInfo.timestamp=2021-05-28%20Friday_06%3A36_pm&pageInfo.fullUrl=https%3A%2F%2Fwww.aircanada.com%2Fus%2Fen%2Faco%2Fhome.html&userInfo.authState=guest&userInfo.ado.category=&userInfo.ado.categoryID=&userInfo.ado.agencyID=&userInfo.ado.agentID=&userInfo.aco.userID=&userInfo.aco.category=&userInfo.aco.emailID=&userInfo.aco.postalCode=&userI

		nfo.aco.loginMethod=&userInfo.aco.persistentLogin=&userInfo.aco.seatPreference=&userInfo.aco.birthMonth=&userInfo.aco.birthYear=&userInfo.aco.countryOfResidence=&userInfo.aco.mrc=&userInfo.aco.amh_flag=&userInfo.aco.ch_flag=&userInfo.aco.th_flag=&mboxMCSDID=7D244856358B2C6A-21C25F992F1C866C&vst.trk=metrics.aircanada.com&vst.trks=smetrics.aircanada.com&mboxMCGVID=90463469790075083520125761519295052389	
http://bloglines.com	Mailchimp	https://downloads.mailchimp.com/js/signup-forms/popup/unique-methods/embed.js	https://d1zgderxoe1a.cloudfront.net/
http://digitalmusicnews.com	Mailchimp	https://downloads.mailchimp.com/js/signup-forms/popup/embed.js	https://d1zgderxoe1a.cloudfront.net/
http://stonetemple.com	Stackpath	https://cdn.shareaholic.net/assets/pub/shareaholic.js	https://k4z6w9b5.stackpathcdn.com/
http://wegmans.com	Adobe	https://mbox.wegmans.com/rest/v1/delivery?client=wegmans&sessionId=8fe5b4e5ef614707b04cbf903b5cda9a&version=2.3.2	https://wegmans.tt.omtrdc.net/
http://bitdefender.com	Adobe	https://starget.bitdefender.com/rest/v1/delivery?client=bitdefender&sessionId=2390290611b649008dcbcbcdb0e73ffc&version=2.5.0	https://stargetbitdefender.tt.omtrdc.net/
http://books.simonandschuster.com	Extole	https://share.simonandschuster.com/core.js	https://simon-and-schuster.extole.io/
http://ultimate-guitar.com	Yandex	https://mc.yandex.ru	https://mc.yandex.com/watch/18746557?wmode=7&page-url=https%3A%2F%2Fwww.ultimate-guitar.com%2F&charset=utf-8&browser-info=pv%3A1%3Agdpr%3A14%3Avf%3Aaldhbh95bz4klu53%3Afp%3A2019%3Afu%3A0%3Aen%3Autf-8%3Ala%3Aen-US%3Av%3A591%3Acn%3A1%3Adp%3A0%3Als%3A547872613012%3Ahid%3A997702020%3Az%3A-420%3Ai%3A20210717120628%3Aet%3A1626548789%3Ac%3A1%3Arn%3A255733658%3Arqn%3A1%3Au%3A1

			626548789376205272%3Aw%3A1213x789%3As%3A1504x1003x24%3Ask%3A1.5%3Ans%3A1626548786007%3Ads%3A58%2C74%2C206%2C92%2C1026%2C0%2C%2C154%2C%2C%2C%2C%2C%3Adsn%3A58%2C75%2C206%2C0%2C1026%2C898%2C%2C183%2C%2C%2C%2C%2C%2C%3Arqnl%3A1%3Afip%3Aac3e153c4e3eb74c56e9d8d3db49706f-a81f3b9bcdd80a361c14af38dc09b309-a81f3b9bcdd80a361c14af38dc09b309-08cddc828a0a4cecdead9052886a5778-6456f00690ac9fc94dca4eb4fd6d061a-9b01b6a68dffdd86560f187ebe2649ec-61b9878bbce18de73aafc8582a198c0c-65112a363b745b2811c7267d45779933-a81f3b9bcdd80a361c14af38dc09b309-c6d7b47b2dcff33f80cab17f3a360d0b-8f94aaac7063d09db7443126fff264fc%3Ati%3A2%3Ast%3A1626548789%3At%3AULTIMATE%20GUITAR%20TABS%20-%201%2C100%2C000%20songs%20catalog%20with%20free%20Chords%2C%20Guitar%20Tabs%2C%20Bass%20Tabs%2C%20Ukulele%20Chords%20and%20Guitar%20Pro%20Tabs!` |
http://harley-davidson.com	Adobe	https://atarget.harley-davidson.com/rest/v1/delivery?client=harleydavidson&sessionId=cbfb4b34bf724662a52f50fa8f830594&version=2.3.3	https://harleydavidson.tt.omtrdc.net/
http://latrobe.edu.au	Adobe	https://starget.latrobe.edu.au/m2/latrobe/mbox/json?mbox=target-global-mbox&mboxSession=aab31cddd9a74f1f882c9367550cbe0d&mboxPC=	https://latrobe.tt.omtrdc.net/

		&mboxPage=d895838ad95444fdbbc0df342862f00c&mboxRid=213af32ed21c4e168f69051d38a32e93&mboxVersion=1.8.0&mboxCount=1&mboxTime=1622672917154&mboxHost=www.latrobe.edu.au&mboxURL=https%3A%2F%2Fwww.latrobe.edu.au%2F&mboxReferrer=&mboxXDomain=enabled&browserHeight=789&browserWidth=1213&browserTimeOffset=-420&screenHeight=1003&screenWidth=1504&colorDepth=24&devicePixelRatio=1.5&screenOrientation=landscape&webGLRenderer=ANGLE%20(Intel(R)%20Iris(R)%20Plus%20Graphics%20Direct3D11%20vs_5_0%20ps_5_0)&mboxMCSDID=149170EE66C11468-40E4C06CC221BB75&vst.trk=metrics.latrobe.edu.au&vst.trks=smetrics.latrobe.edu.au&mboxMCGVID=76229748377754704239014239423653213975	
http://abqjournal.com	Mailchimp	https://downloads.mailchimp.com/js/signup-forms/popup/unique-methods/embed.js	https://d1zgderxoe1a.cloudfront.net/
http://siriusxm.com	Adobe	https://metrics-target.siriusxm.com/m2/siriusxmradio/mbox/json?mbox=target-global-mbox&mboxSession=b678490277ce4939af4a0356d39462d3&mboxPC=&mboxPage=180b8ac00a2643a0a0e5b66806ae131a&mboxRid=817f09120f1e40f0b28f2ce520b13a11&mboxVersion=1.8.2&mboxCount=1&mboxTime=1622758103008&mboxHost=www.siriusxm.com&mboxURL=https%3A%2F%2Fwww.siriusxm.com%2F&mboxReferrer=&browserHeight=789&browserWidth=1213&browserTimeOffset=-420&screenHeight=1003&screenWidth=1504&colorDepth=24&devicePixelRatio=1.5&screenOrientation=landscape&webGLRenderer=ANGLE%	https://siriusxmradio.tt.omtrdc.net/

		20(Intel(R)%20Iris(R)%20Plus%20Graphics%20Direct3D11%20vs_5_0%20ps_5_0)&isPhoenix=true&sxCookieBanner=&profile.adobeQA=%25adobeQA%25&profile.marketType=&profile.userPromoCode=%25Non-PII%20SubPromoCode%25&profile.calculatedSegment=%5B%22acctDefault%22%2C%22contDefault%22%2C%22mktgDefault%22%5D&mboxMCSDID=6B4991B27EDF268B-439679B459BA9ACD&mboxMCGVID=67790027044781669810744818922715308823	
http://nationwide.com	Adobe	https://target.nationwide.com/rest/v1/delivery?client=nationwideinsurance&sessionId=3269b77327a14f2680a089130c8e4971&version=2.4.1	https://nationwideinsurance.tt.omtrdc.net
http://casino.org	Clicky	https://sa.casino.org/js	https://sa.casino.org.re.getclicky.com/
http://jihadwatch.org	Stackpath	https://cdn.shareaholic.net/assets/pub/shareaholic.js	https://k4z6w9b5.stackpathcdn.com/
http://deakin.edu.au	Adobe	https://stt.deakin.edu.au/rest/v1/delivery?client=deakinuniversity&sessionId=2fb5a13d117a46bababb871f89074b52&version=2.4.1	https://deakinuniversity.tt.omtrdc.net/
http://coolhunting.com	Mailchimp	https://downloads.mailchimp.com/js/signup-forms/popup/unique-methods/embed.js?_=1622871689639	https://d1zgderxoe1a.cloudfront.net/
http://architectureartdesigns.com	Stackpath	https://cdn.shareaholic.net/assets/pub/shareaholic.js	https://k4z6w9b5.stackpathcdn.com/
http://focusonthefamily.com	Matomo (formerly known as Piwik)	https://epiphany.masterworks.com/containers/45954263-b894-48fc-b0bb-40979513431a.js	https://piwik.pro.us-east-1.piwik.pro/

Table 4. Sites found using unconsented third-party and CNAME trackers, including alias and actual tracking URLs.