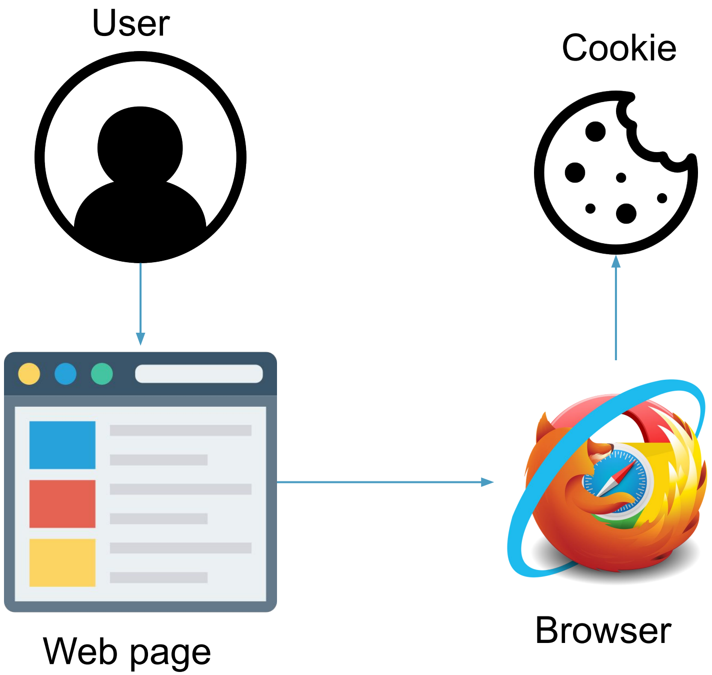
Circumvention of tracking protections by means of first-party tracking

Yana Dimova, Gunes Acar, Lukasz Olejnik, Wouter Joosen, Tom Van Goethem

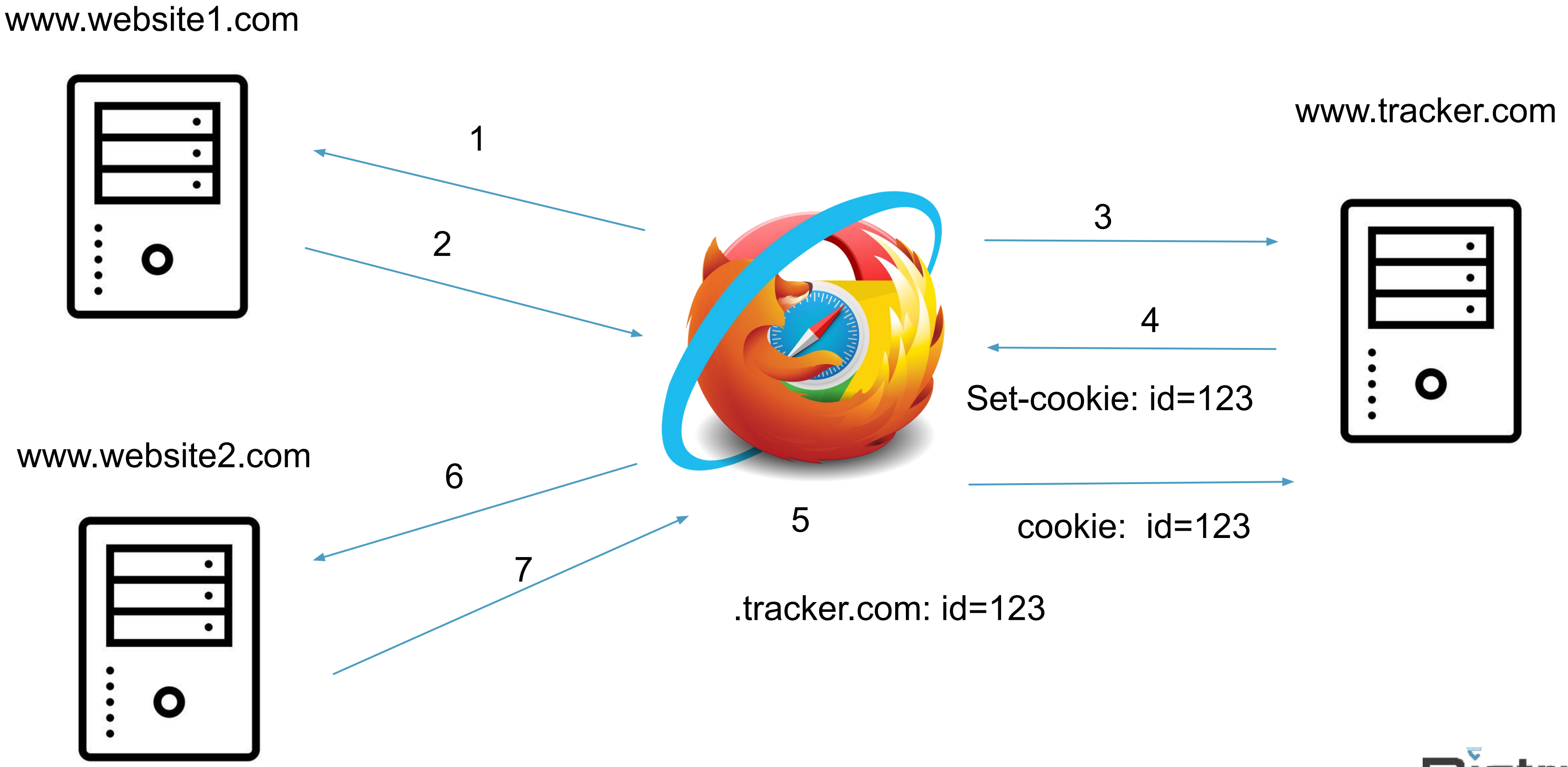
DistriNet

Online tracking



- Session cookies
  - Essential
  - First-party
  - Provide functionality
- Tracking cookies
  - Unique identifier
  - Can be first-party of third-party
- Same-origin policy
  - Security measure
  - Prevent resource access

Third-party tracking



www.website1.com

www.tracker.com

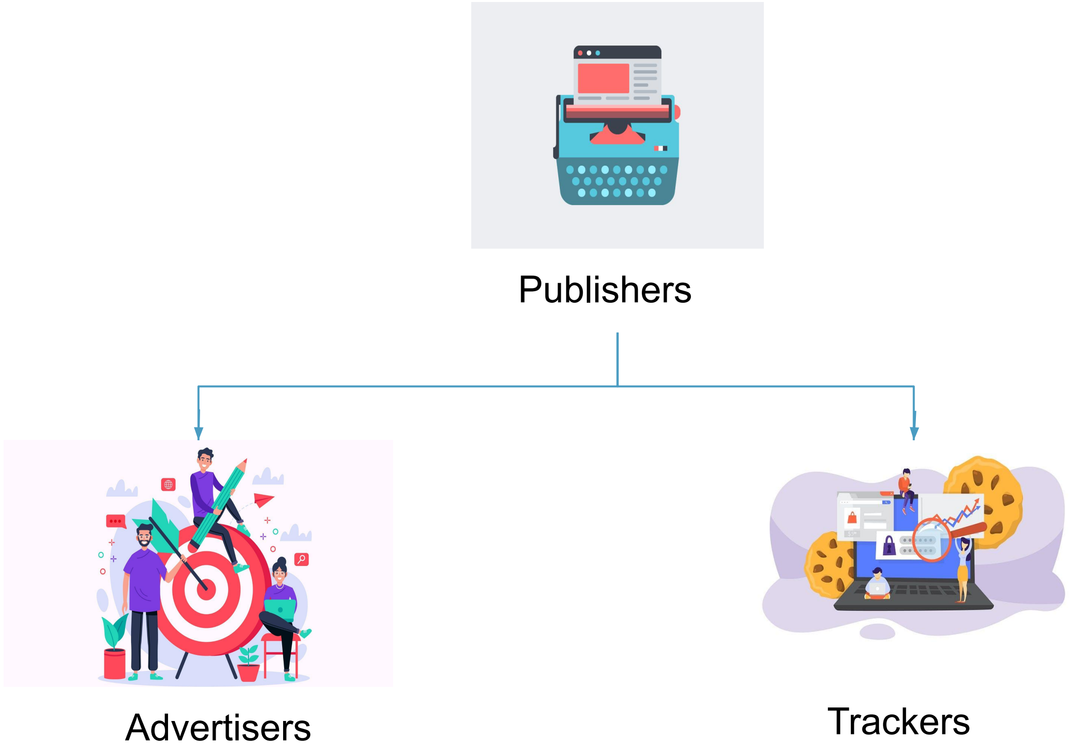
www.website2.com

Set-cookie: id=123

cookie: id=123

.tracker.com: id=123

Key Players

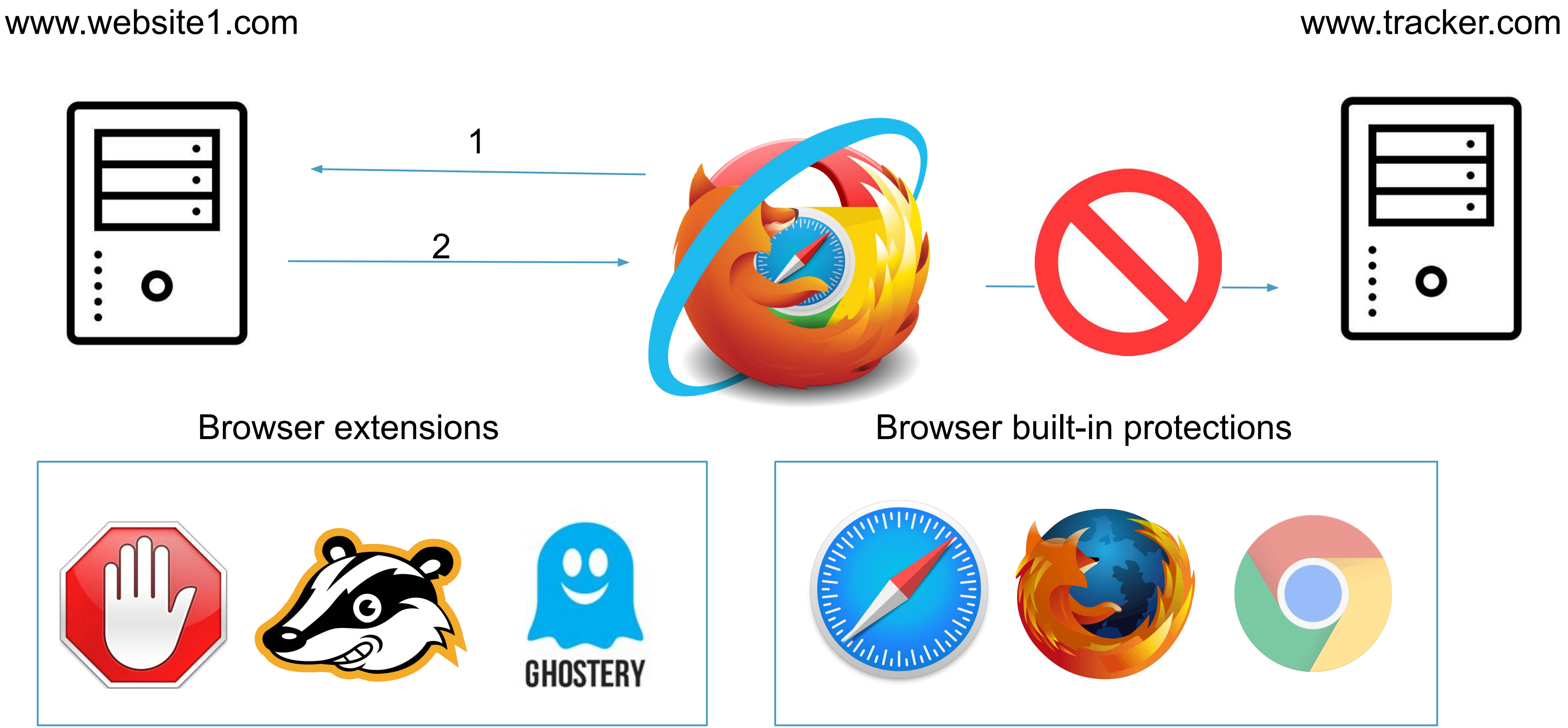


Publishers

Advertisers

Trackers

Third-party tracking



Browser extensions

Browser built-in protections

Key Players

Publishers

Trackers

Advertisers

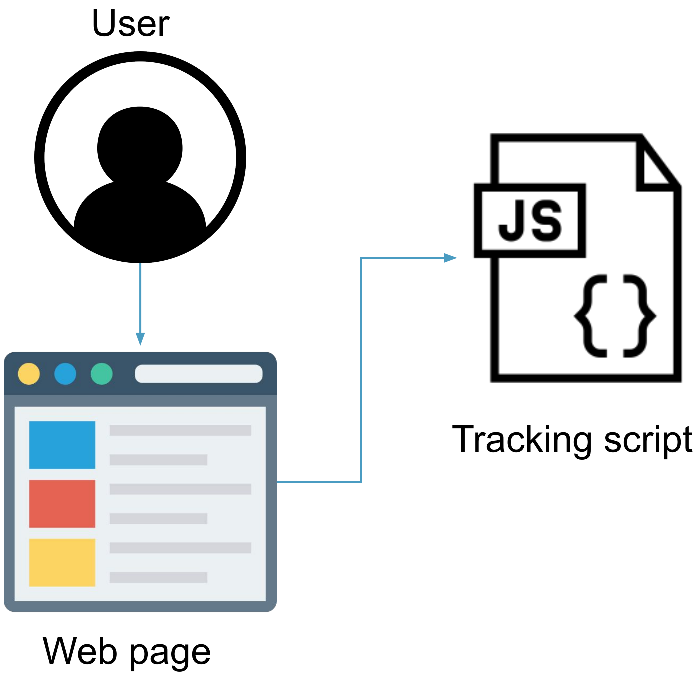
vs.

Users

Browsers

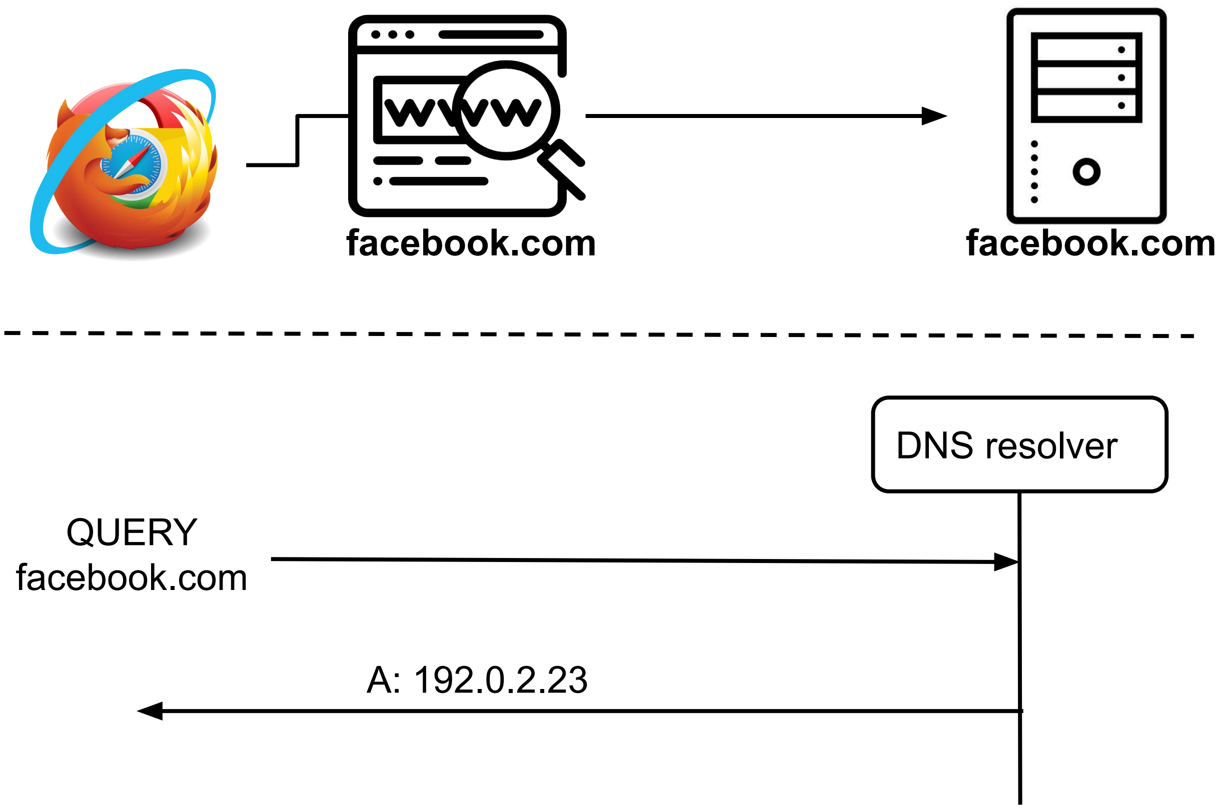
Privacy protections

First-party tracking



- As a circumvention of cookie blocking
- First-party cookie
- Same-site
  - Insights on user behavior
- In combination with persistent tracking

DNS



facebook.com

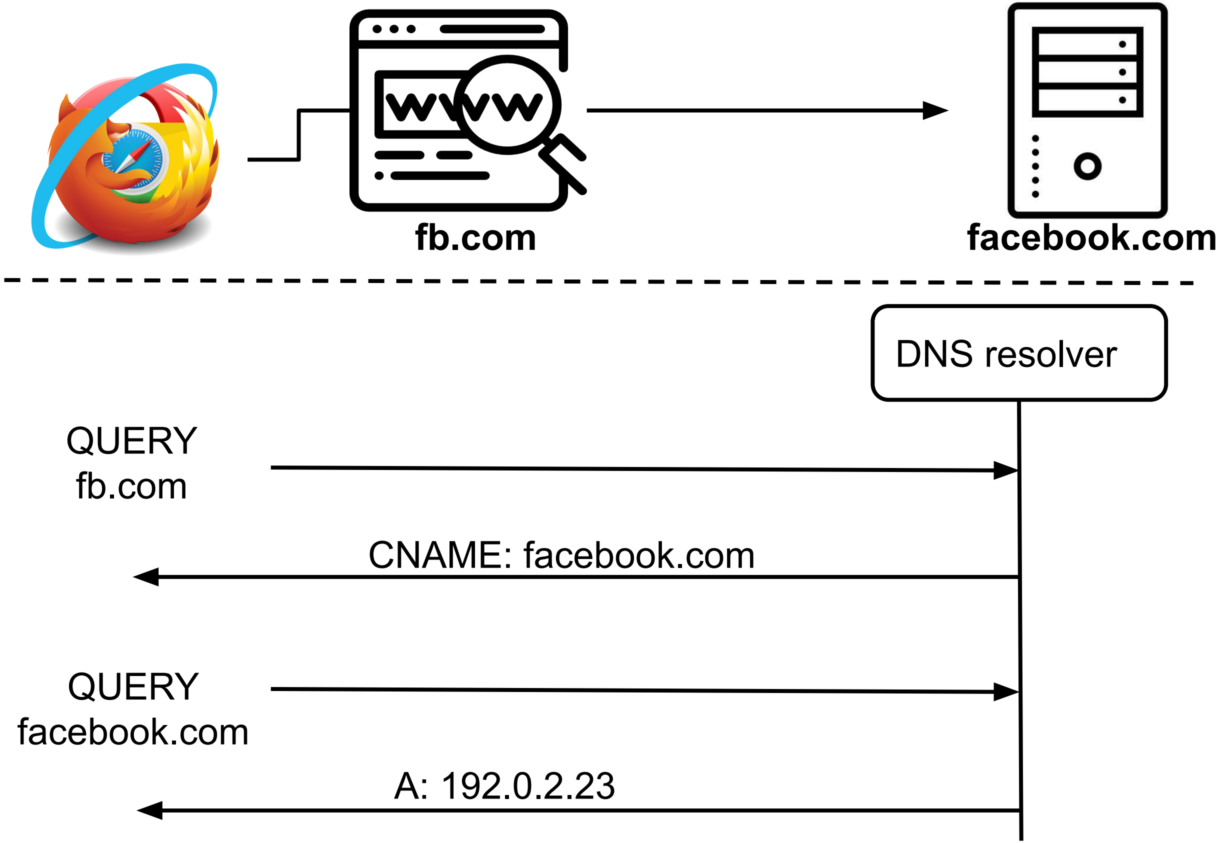
facebook.com

DNS resolver

QUERY
facebook.com

A: 192.0.2.23

DNS



fb.com

facebook.com

DNS resolver

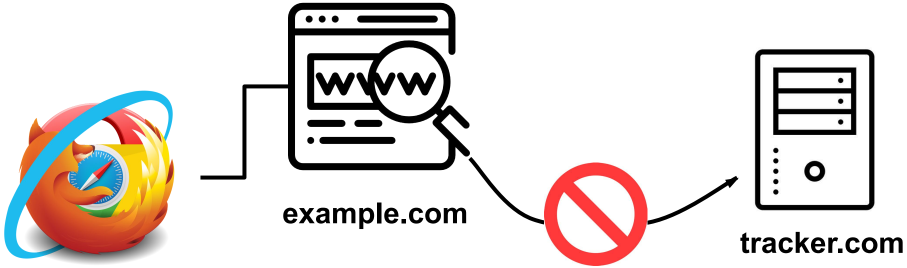
QUERY
fb.com

CNAME: facebook.com

QUERY
facebook.com

A: 192.0.2.23

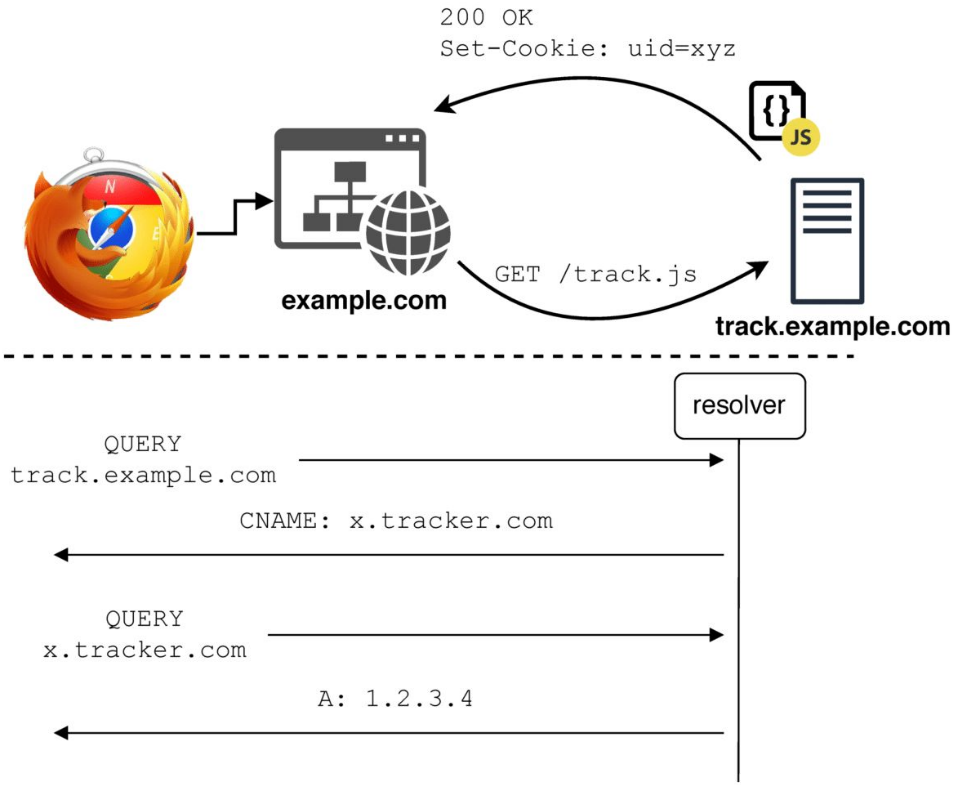
Third-party tracking



example.com

tracker.com

CNAME-based tracking



```
200 OK
Set-Cookie: uid=xyz
```

example.com

```
GET /track.js
```

track.example.com

resolver

```
QUERY
track.example.com
```

```
CNAME: x.tracker.com
```

```
QUERY
x.tracker.com
```

```
A: 1.2.3.4
```

Detecting CNAME-based tracking

Methodology

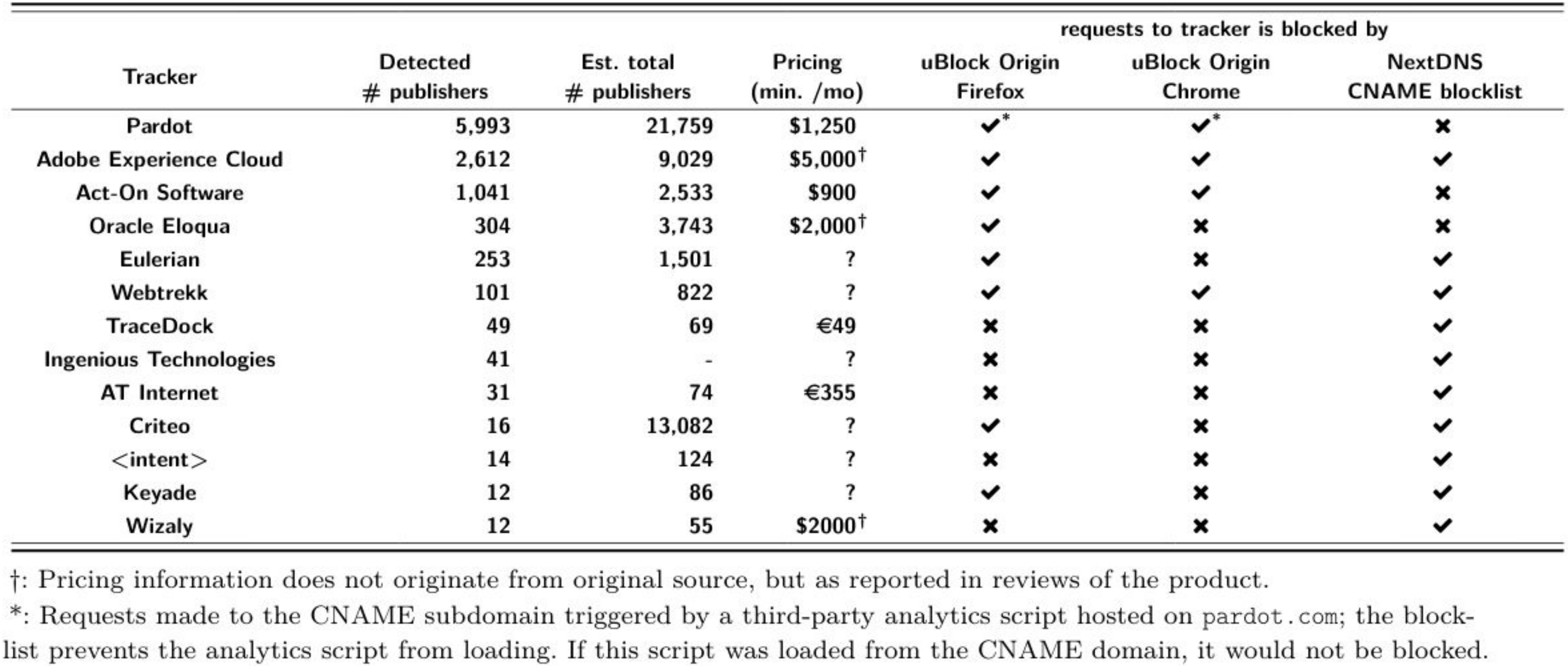
- Step 1: CNAME records
  - First party points to third party
- Step 2: Dataset
  - Starting from HTTP Archive (5.6M frequently-visited websites) dataset
  - First-party requests to subdomain

List of CNAME tracker candidates

Methodology

- Step 3: Filter non-tracking candidates
    - Manual analysis
    - Analyse candidate website for references to tracking or features that would require tracking
    - 13 manually-verified trackers
    - Tracker-specific fingerprint
- Step 4: Validation
    - Run crawl with other user agent (Safari)
    - Found tracker that only did tracking for Safari users

Results

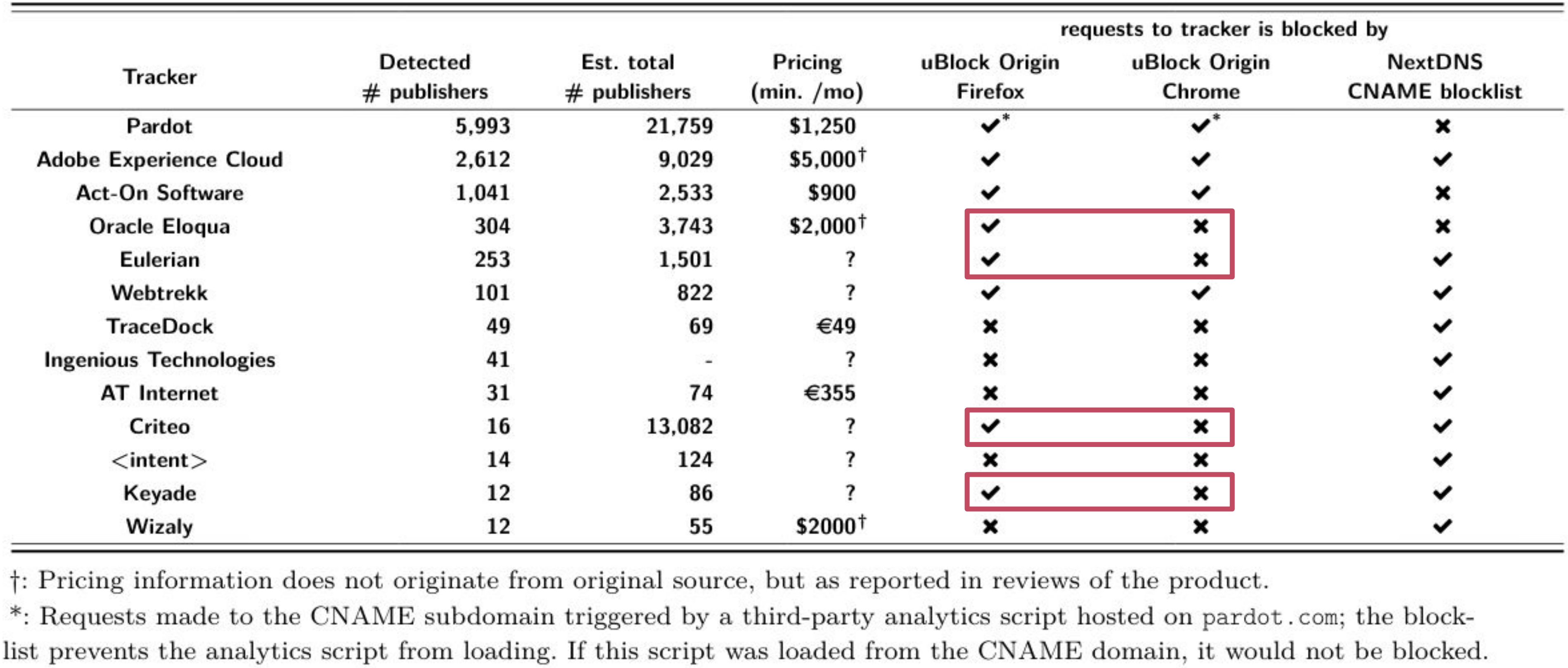


Tracker	Detected # publishers	Est. total # publishers	Pricing (min. /mo)	requests to tracker is blocked by uBlock Origin Firefox	 uBlock Origin Chrome	 NextDNS CNAME blocklist
Pardot	5,993	21,759	$1,250	✓*	✓*	✗
Adobe Experience Cloud	2,612	9,029	$5,000†	✓	✓	✓
Act-On Software	1,041	2,533	$900	✓	✓	✗
Oracle Eloqua	304	3,743	$2,000†	✓	✗	✗
Eulerian	253	1,501	?	✓	✗	✓
Webtrekk	101	822	?	✓	✓	✓
TraceDock	49	69	€49	✗	✗	✓
Ingenious Technologies	41	-	?	✗	✗	✓
AT Internet	31	74	€355	✗	✗	✓
Criteo	16	13,082	?	✓	✗	✓
<intent>	14	124	?	✗	✗	✓
Keyade	12	86	?	✓	✗	✓
Wizaly	12	55	$2000†	✗	✗	✓

†: Pricing information does not originate from original source, but as reported in reviews of the product.

*: Requests made to the CNAME subdomain triggered by a third-party analytics script hosted on `pardot.com`; the blocklist prevents the analytics script from loading. If this script was loaded from the CNAME domain, it would not be blocked.

Results

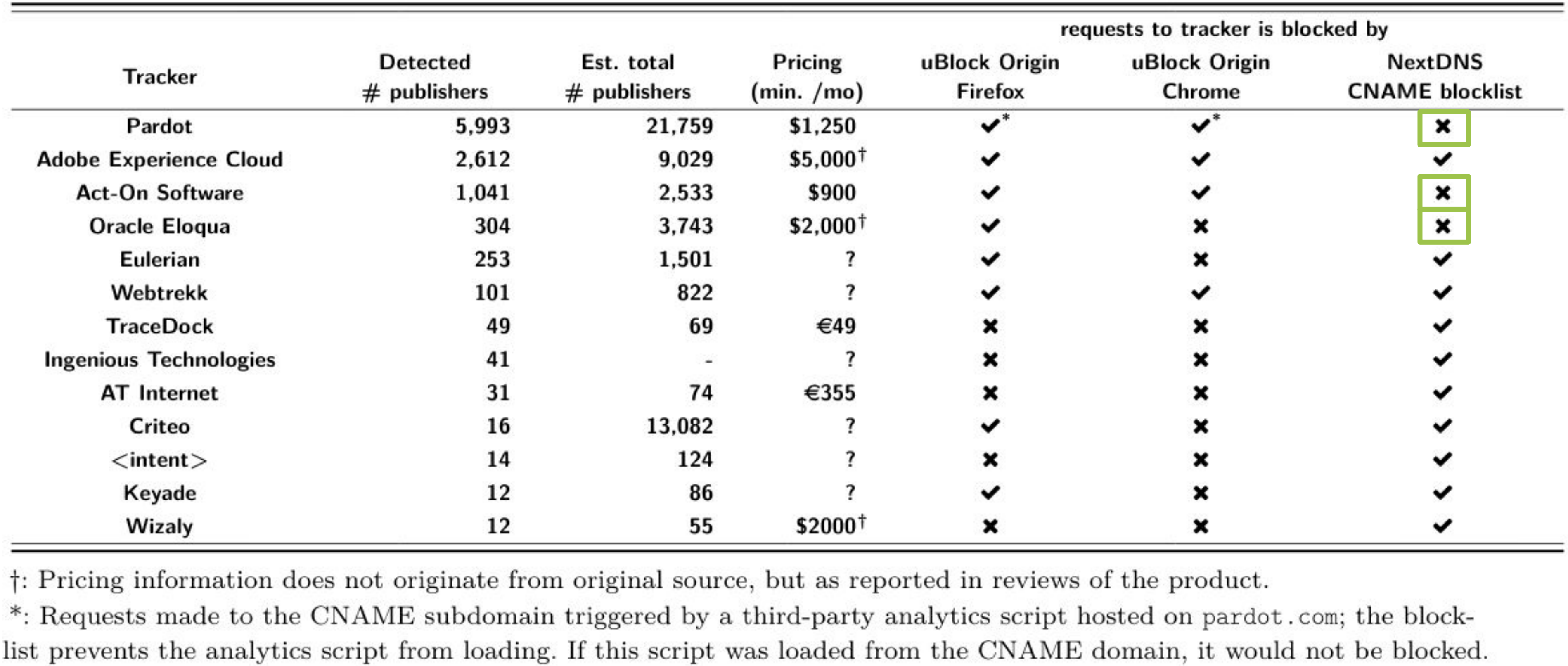


				requests to tracker is blocked by		
Tracker	Detected # publishers	Est. total # publishers	Pricing (min. /mo)	uBlock Origin Firefox	uBlock Origin Chrome	NextDNS CNAME blocklist
Pardot	5,993	21,759	$1,250	✓[*]	✓[*]	✗
Adobe Experience Cloud	2,612	9,029	$5,000[†]	✓	✓	✓
Act-On Software	1,041	2,533	$900	✓	✓	✗
Oracle Eloqua	304	3,743	$2,000[†]	✓	✗	✗
Eulerian	253	1,501	?	✓	✗	✓
Webtrekk	101	822	?	✓	✓	✓
TraceDock	49	69	€49	✗	✗	✓
Ingenious Technologies	41	-	?	✗	✗	✓
AT Internet	31	74	€355	✗	✗	✓
Criteo	16	13,082	?	✓	✗	✓
<intent>	14	124	?	✗	✗	✓
Keyade	12	86	?	✓	✗	✓
Wizaly	12	55	$2000[†]	✗	✗	✓

†: Pricing information does not originate from original source, but as reported in reviews of the product.

*: Requests made to the CNAME subdomain triggered by a third-party analytics script hosted on `pardot.com`; the blocklist prevents the analytics script from loading. If this script was loaded from the CNAME domain, it would not be blocked.

Results

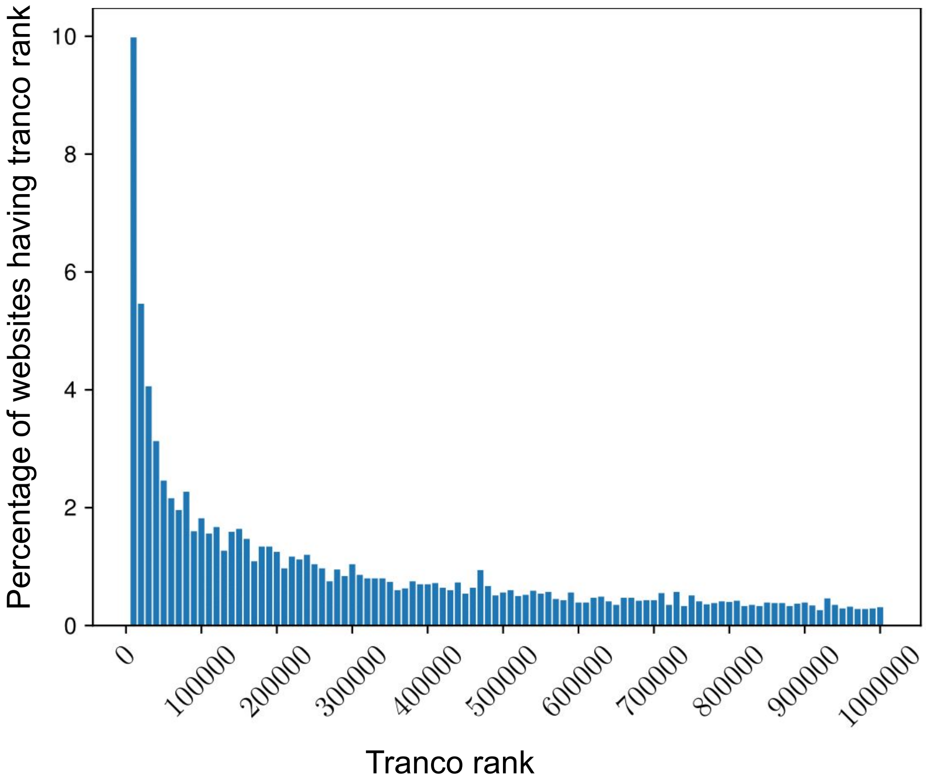


Tracker	Detected # publishers	Est. total # publishers	Pricing (min. /mo)	requests to tracker is blocked by uBlock Origin Firefox	 uBlock Origin Chrome	 NextDNS CNAME blocklist
Pardot	5,993	21,759	$1,250	✓*	✓*	✗
Adobe Experience Cloud	2,612	9,029	$5,000†	✓	✓	✓
Act-On Software	1,041	2,533	$900	✓	✓	✗
Oracle Eloqua	304	3,743	$2,000†	✓	✗	✗
Eulerian	253	1,501	?	✓	✗	✓
Webtrekk	101	822	?	✓	✓	✓
TraceDock	49	69	€49	✗	✗	✓
Ingenious Technologies	41	-	?	✗	✗	✓
AT Internet	31	74	€355	✗	✗	✓
Criteo	16	13,082	?	✓	✗	✓
<intent>	14	124	?	✗	✗	✓
Keyade	12	86	?	✓	✗	✓
Wizaly	12	55	$2000†	✗	✗	✓

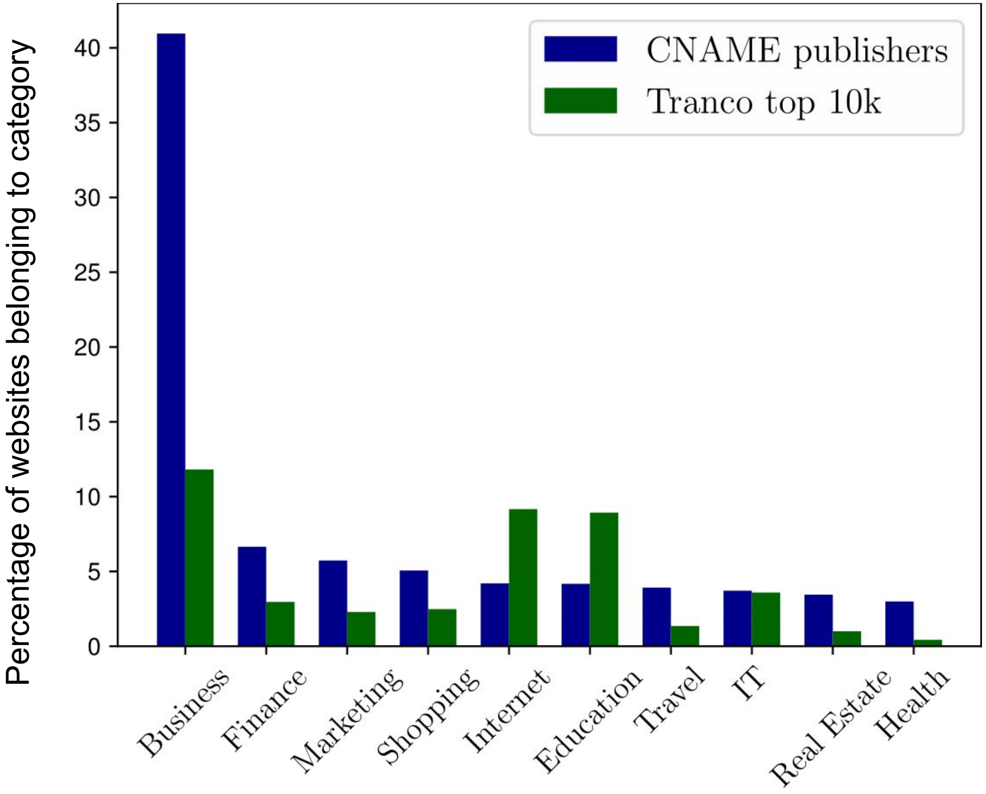
†: Pricing information does not originate from original source, but as reported in reviews of the product.

*: Requests made to the CNAME subdomain triggered by a third-party analytics script hosted on pardot.com; the blocklist prevents the analytics script from loading. If this script was loaded from the CNAME domain, it would not be blocked.

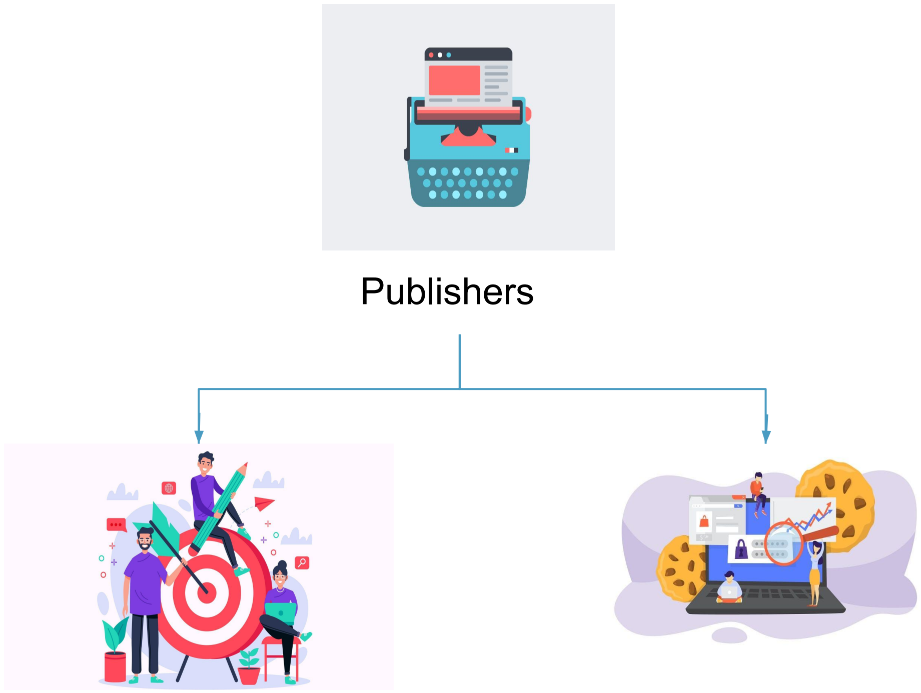
Popularity of publishers using CNAME-based tracking



Categories of publishers using CNAME-based tracking



Key Players



Publishers

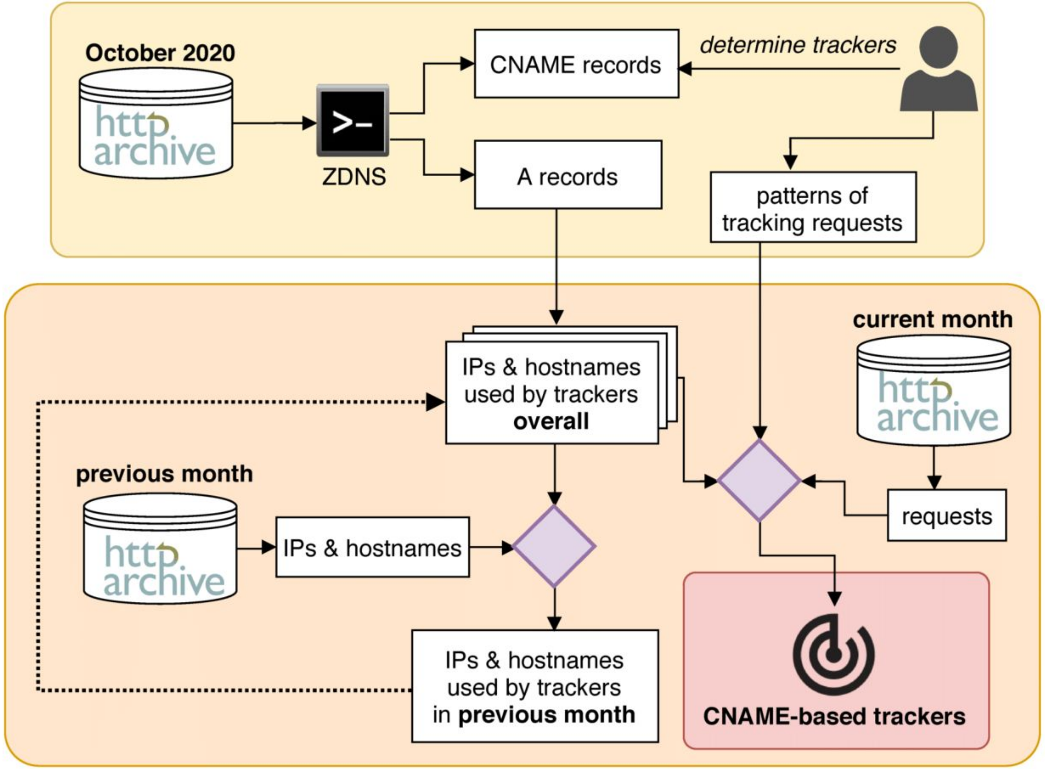
Advertisers

Trackers

- 10 474 publishers
  - Mostly businesses
  - 9.98% in Tranco top 10k
- 13 CNAME-based trackers
  - Varying size
  - Previously unknown

Historical evolution of CNAME-based tracking

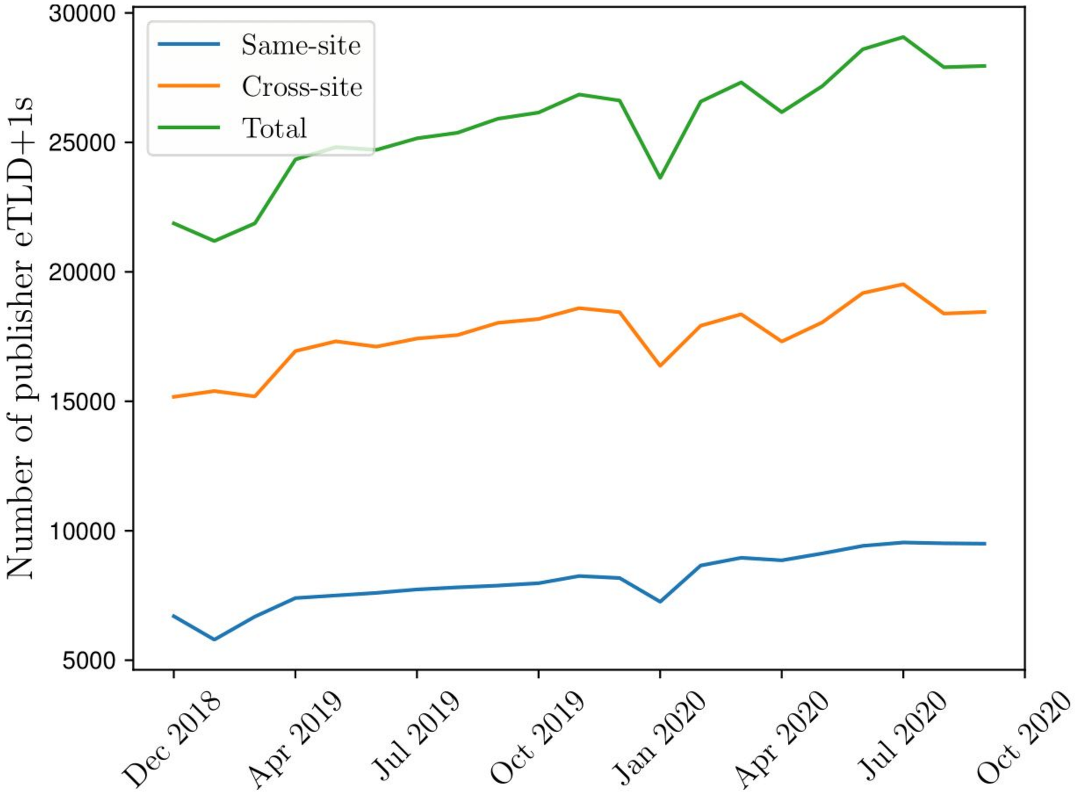
Methodology



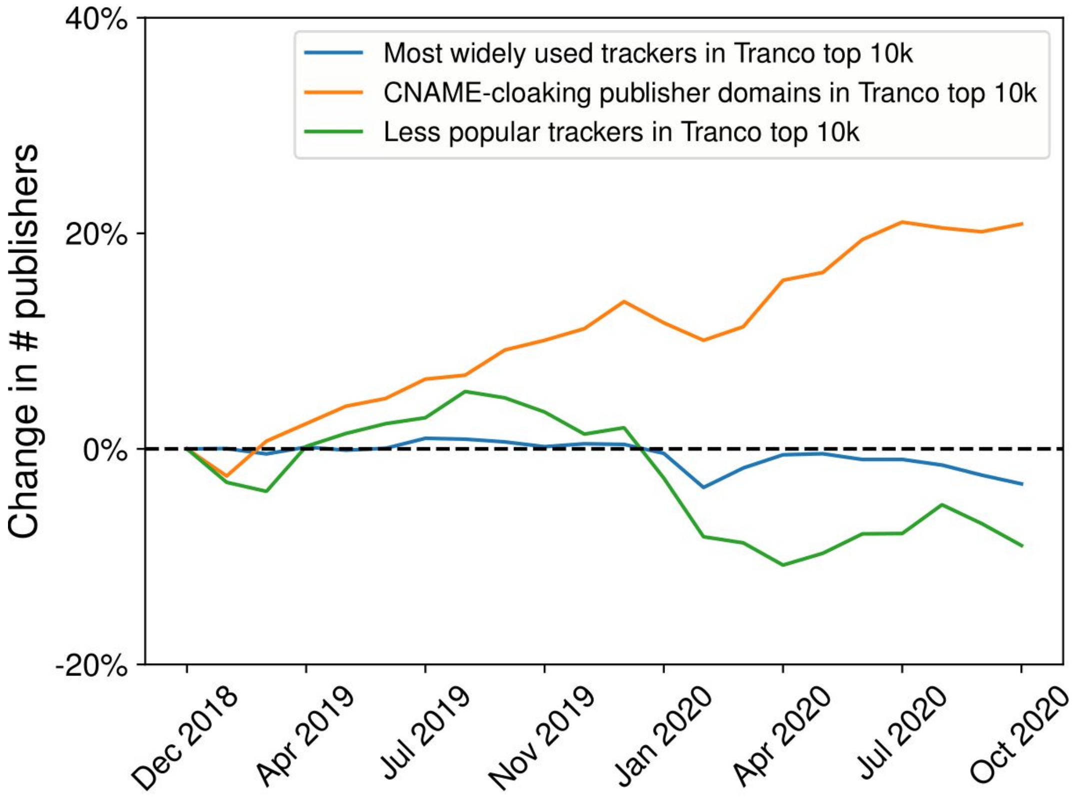
› Public dataset
  - HTTP Archive

› Recursive approach

Historical Analysis



Comparison to third-party tracking



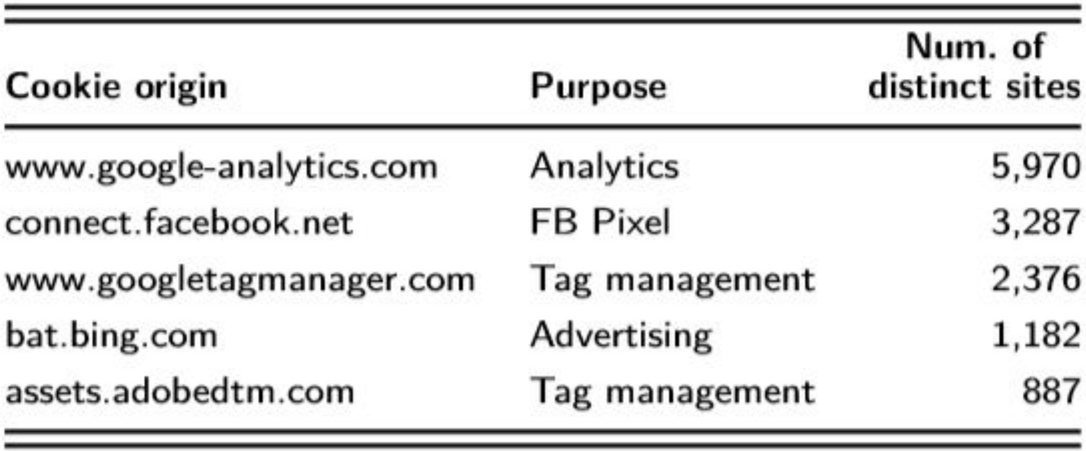
Effects on third-party tracking

- Evolution of third-party tracking
- Recent CNAME publisher websites
  - 6 months non-active/6 consecutive months active
  - Number of third-parties unchanged
  - Complimentary basis

Implications of CNAME-based tracking

Privacy

- Cookie leaks
  - Cookies scoped to domain of website
  - 8807 sites using CNAME-based tracking
  - Cookies leaking on 95% sites



Cookie origin	Purpose	Num. of distinct sites
www.google-analytics.com	Analytics	5,970
connect.facebook.net	FB Pixel	3,287
www.googletagmanager.com	Tag management	2,376
bat.bing.com	Advertising	1,182
assets.adobedtm.com	Tag management	887

Privacy

- Cookies leaking in request URLs
  - Cookie syncing
  - Bypass tracking protections
  - Set by third-party domain of the tracker

Privacy

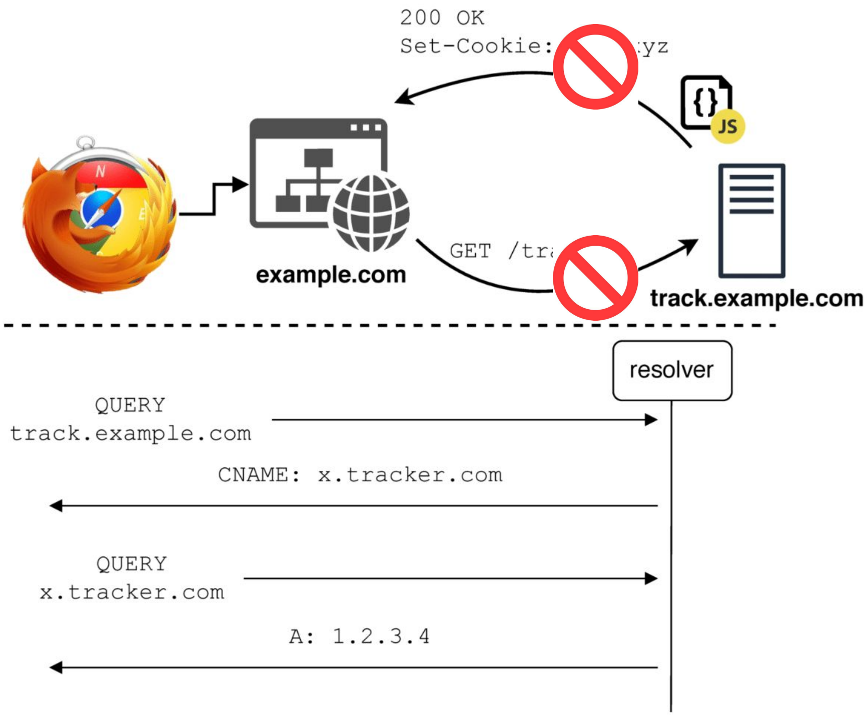
- Leaking of sensitive information from cookies
- Manual analysis on 50 websites
  - Full name (1 website)
  - Location (2 websites)
  - Email (4 websites)
  - Authentication cookie (10 websites)

Security

- Issues arising from the CNAME-based tracking scheme
- Tracker included in first-party context
- Two major vulnerabilities affecting all publisher websites

Countermeasures

- DNS-level blocking
- Limited cookie lifetime



Conclusion

- Methodology allows to detect previously unknown CNAME-based trackers
- Large-scale evaluation of CNAME-based tracking
  - Increased in popularity by 21%
- Privacy and security issues
  - Two major web security flaws
  - Sensitive information leaking

DistriNet

Thank you!

https://distrinet.cs.kuleuven.be/