Watching them Watching us

Konark Modi | @konarkmodi
Santiago Saavedra | @ssice
Sofía Prósper | @sofipros

github.com/cliqz-oss/local-sheriff

trackula.org
Top 5 trackers in Europe

Google: 81%
Facebook: 27%
Amazon: 17%
Criteo: 9%
INFOOnline: 9%
Microsoft: 8%

Source: whotracks.me from December 2018
How does it work?
How does it work?
How does it work?
How does it work?
How does it work?
How does it work?
How does it work?
How does it work?
LOCAL SHERIFF
A URL which contains sensitive information or can lead to a page which contains sensitive information
From all of us at Mozilla

Thank you

We're working hard to protect the open web. We want to keep you in the loop!

konark@cliqz.com

I'm okay with Mozilla handling my info as explained in this Privacy Policy.

Sign up now
IDENTIFYING LEAKS
Have any of the data points entered in forms been shared?

Input information which should not have been shared without consent with services you have not interacted with. Like Email address, Phone number, Name, Address etc.

=konark@cliqz.com

7 third-party domains owned by 2 different companies courtesy 1 website.

<table>
<thead>
<tr>
<th>Company</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>donate.mozilla.org</td>
</tr>
<tr>
<td>Unknown</td>
<td>donate.mozilla.org</td>
</tr>
</tbody>
</table>

Detailed Logs

https://donate.mozilla.org/en-US/thank-you/?paymentMethod=Stripe&amount=200&currency=USD&str_id=ch_dmtTMk0Vg2xhxtmqyUIOLp&str_frequency=one-time&email=konark@cliqz.com&country=Germany&locale=en-US&k=1&k=1&k=1

Visit Page

Google


Unknown

maxcdn.bootstrapcdn.com, bootstrapcdn.com, checkout.stripe.com, c.shnp.org
Your tickets have been sent to modi.konark@gmail.com

FRIDAY
3 AUG
09:47 München Hbf
15:56

09:47 München Hbf (Munich, Main Station)
13:40 Frankfurt (Main) Hbf (Main Station)
14:49 Frankfurt (Main) Hbf (Main Station)
15:56 Marburg (Lahn)

€111.80

Ticket reference:

SUNDAY
5 AUG
13:58 Marburg (Lahn)
18:56 München Hbf

13:58 Marburg (Lahn)
15:11 Kassel-Wilhelmshöhe

Proof of payment
Purchased on 07 July 2018

€111.00

Refund and exchange: Sparpreis

Refund and exchange: Sparpreis
trainline.eu/order/3e5

has been leaked to **17 third-party domains**, owned by **5 different companies** courtesy **1 website**.

<table>
<thead>
<tr>
<th>Company</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td><a href="http://www.trainline.eu">www.trainline.eu</a></td>
</tr>
<tr>
<td>Google</td>
<td><a href="http://www.trainline.eu">www.trainline.eu</a></td>
</tr>
<tr>
<td>Microsoft</td>
<td><a href="http://www.trainline.eu">www.trainline.eu</a></td>
</tr>
<tr>
<td>ThreatMetrix</td>
<td><a href="http://www.trainline.eu">www.trainline.eu</a></td>
</tr>
<tr>
<td>New Relic</td>
<td><a href="http://www.trainline.eu">www.trainline.eu</a></td>
</tr>
</tbody>
</table>
You are logged in as **order # 807**
Ticket Email: **modi.konark**

**Cancellation / name change # 80751**
4 Aug., 05:00 Munich central bus station → Innsbruck Südbahnstraße

**Konark modes**
Mobile phone number: **+4976**

or

- [ ] Cancel entire booking

or

- [ ] Change billing address
Request URL: https://fonts.googleapis.com/css?family=PT+Sans+Narrow:400,700
Request Method: GET
Status Code: 200
Remote Address: [2a00:1450:4001:821::200a]:443
Referrer Policy: no-referrer-when-downgrade

Response Headers (15)

Request Headers

⚠️ Provisional headers are shown
Referrer: https://shop.flixbus.de/rebooking/mobile/auth?orderId=807----------h=54xy6dheevs52d----------hscnjqdwu91q990
Your Booking:

For flights to the USA, airlines are legally obliged to transmit passenger data to the US authorities via the Advance Passenger Information System (APIS). This rule does not apply to passengers with a permanent resident permit ('green card') or to transit passengers. You can enter your APIS data below.

If you hold a visa for the country of your destination please also enter the information below.

**Visa and immigration data (APIS)**

**Passenger 1 (Adult):**

**Personal details**
- First name
- Last name
- Gender
- Date of Birth

**Form of identification**
How is this person going to identify himself/herself at immigration?
- Document
- Expiry date
- Document number
- Issuing country
## Identifying Leaks

The token `0339651b1` has been leaked to **4 third-party domains**, owned by **4 different companies** courtesy **2 websites**.

<table>
<thead>
<tr>
<th>Company</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td><a href="http://www.lufthansa.com">www.lufthansa.com</a></td>
</tr>
<tr>
<td>Google</td>
<td>book.lufthansa.com</td>
</tr>
<tr>
<td>Oracle Maxymiser</td>
<td>book.lufthansa.com</td>
</tr>
<tr>
<td>Webtrends</td>
<td>book.lufthansa.com</td>
</tr>
<tr>
<td>Exactag</td>
<td>book.lufthansa.com</td>
</tr>
</tbody>
</table>

### Detailed Logs

Leaked url via ref or a key like ci/dr in third-party:


Telltale URL
Kontoübersicht

Profil
Benutzername
E-Mail
Geburtsdatum
Land
DE

Spotify Free

PREMIUM HOLEN

Überall abmelden
Meide Dich überall dort ab, wo Du Spotify geöffnet hast, etwa im Internet, auf dem Handy, dem Computer oder anderen Geräten.

ÜBERALL ABMELDEN
<table>
<thead>
<tr>
<th>Request</th>
<th>Response</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host:</strong></td>
<td>sb.scorecardresearch.com</td>
<td></td>
</tr>
<tr>
<td><strong>Connection:</strong></td>
<td>keep-alive</td>
<td></td>
</tr>
<tr>
<td><strong>User-Agent:</strong></td>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.146 Safari/537.36 OPR/52.0.2871.20 (Edition beta)</td>
<td></td>
</tr>
<tr>
<td><strong>Accept:</strong></td>
<td>image/webp,image/apng,image/<em>,</em>/*;q=0.8</td>
<td></td>
</tr>
<tr>
<td><strong>Referer:</strong></td>
<td><a href="https://www.spotify.com/de/account/overview/?utm=NAphCkkKDvNwb3RpZnktdXNlcnMSCmVbM3yMxMMDMaA5gUL4shlV1rpBMCA">https://www.spotify.com/de/account/overview/?utm=NAphCkkKDvNwb3RpZnktdXNlcnMSCmVbM3yMxMMDMaA5gUL4shlV1rpBMCA</a></td>
<td></td>
</tr>
<tr>
<td><strong>Accept-Encoding:</strong></td>
<td>gzip, deflate, br</td>
<td></td>
</tr>
<tr>
<td><strong>Accept-Language:</strong></td>
<td>en-GB,en-US;q=0.9,en;q=0.8</td>
<td></td>
</tr>
<tr>
<td><strong>Cookie:</strong></td>
<td>UID=17523a194187173be228dcb1521336255; UIDR=1521336255</td>
<td></td>
</tr>
</tbody>
</table>

**Query**

```
c1: 2
c2: 15654041
ns_t: 1521340042970
ns_c: UTF-8
c8: Kontoubersicht - Spotify
c7: https://www.spotify.com/de/account/overview/?utm_source=sp
b3RpZnktdXNlcnMSCmVbM3yMxMMDMaA5gBASUnxq1aMiICFgQO8xQyPevEhbhV```

**Response Code:** 204 No Content [no content] 2.25s
48.1513886 has been leaked to 18 third-party domains, owned by 7 different companies courtesy 1 website.

<table>
<thead>
<tr>
<th>Company</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td><a href="http://www.foodora.de">www.foodora.de</a></td>
</tr>
<tr>
<td>Google</td>
<td><a href="http://www.foodora.de">www.foodora.de</a></td>
</tr>
<tr>
<td>Amazon</td>
<td><a href="http://www.foodora.de">www.foodora.de</a></td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.foodora.de">www.foodora.de</a></td>
</tr>
<tr>
<td>New Relic</td>
<td><a href="http://www.foodora.de">www.foodora.de</a></td>
</tr>
<tr>
<td>Sift Science</td>
<td><a href="http://www.foodora.de">www.foodora.de</a></td>
</tr>
<tr>
<td>TrackJS</td>
<td><a href="http://www.foodora.de">www.foodora.de</a></td>
</tr>
</tbody>
</table>
OH THE HORROR
RISKS OF TELLTALE URLs #1

Websites are carelessly leaking sensitive PII information to plethora of third-parties
RISKS OF TELLTALE URLS #2

- Websites are carelessly leaking sensitive PII information to plethora of third-parties

- Most often without users' consent
RISKS OF TELLTALE URLS #3

- Websites are carelessly leaking sensitive PII information to plethora of third-parties
- Most often without users’ consent.

More dangerously: Without the websites realizing themselves.

Protecting your details and protecting yourself against internet fraud

Here are some simple steps you can take to ensure your information is kept securely:

- Keep your booking reference confidential - upon making a booking a unique booking reference (also known as a PNR or Passenger Name Record) will appear on the email confirmation or ticket of each person in your booking. It is important that you keep your booking reference confidential at all times. Other persons may be able to access your booking details through our system if you disclose your booking reference to them.

<table>
<thead>
<tr>
<th>Third-party</th>
<th>Leaking via header</th>
<th>Leaking via Query Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>boxever.com</td>
<td>Referer</td>
<td></td>
</tr>
<tr>
<td>googletagmanager.com</td>
<td>Referer</td>
<td></td>
</tr>
<tr>
<td>facebook.com</td>
<td>Referer</td>
<td>DL</td>
</tr>
<tr>
<td>facebook.net</td>
<td>Referer</td>
<td></td>
</tr>
<tr>
<td>google-analytics.com</td>
<td>Referer</td>
<td>DL, DR</td>
</tr>
<tr>
<td>coremetrics</td>
<td>Referer</td>
<td>UL, RF</td>
</tr>
<tr>
<td>ads-twitter.com</td>
<td>Referer</td>
<td></td>
</tr>
<tr>
<td>qubitproducts</td>
<td>Referer</td>
<td></td>
</tr>
<tr>
<td>crazyegg.com</td>
<td>Referer</td>
<td></td>
</tr>
<tr>
<td>ek.aero</td>
<td>Referer</td>
<td></td>
</tr>
<tr>
<td>cloudfront</td>
<td>Referer</td>
<td></td>
</tr>
</tbody>
</table>
EMPOWERING USERS'
LOCAL SHERIFF

1. Monitor all Webrequests that take place in the browser
https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/API/webRequest
2. Classify as first party vs third-party
3. Locally shipped copy of hostnames to Companies

Source: https://whotracks.me
https://github.com/cliqz-oss/whotracks.me
4. Search interface
From all of us at Mozilla

Thank you

We're working hard to protect the open web. We want to keep you in the loop!

Email: konark@cliqz.com

I'm okay with Mozilla handling my info as explained in this Privacy Policy.

Sign up now
Have any of the data points entered in forms been shared?

Input information which should not have been shared without consent with services you have not interacted with. Like Email address, Phone number, Name, Address etc.

=konark@cliqz.com

=konark@cliqz.com

has been leaked to 7 third-party domains owned by 2 different companies courtesy 1 website.

<table>
<thead>
<tr>
<th>Company</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>donate.mozilla.org</td>
</tr>
<tr>
<td>Unknown</td>
<td>donate.mozilla.org</td>
</tr>
</tbody>
</table>

**Detailed Logs**

Detailed logs of visits and transactions related to the email address.

Visit Page
- Google
- Unknown
  - maxthon bootstrap.com, checkout.stripe.com, c.shog.org
facebook.com/tr has been leaked to 1 third-party domains, owned by 1 different companies courtesy 4 website.

<table>
<thead>
<tr>
<th>Company</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td><a href="http://www.lieferando.de">www.lieferando.de</a></td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.nytimes.com">www.nytimes.com</a></td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.thetrainline.com">www.thetrainline.com</a></td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.trainline.eu">www.trainline.eu</a></td>
</tr>
</tbody>
</table>

Also found fr=0Sh6fFpK7USdFh0w3 in third-party urls courtesy shop.flixbus.de:

Cookie fr=0Sh6fFpK7USdFh0w3. Ba5J4E_Fsl.1.0.BbT7LM.
fr=0Sh6fFpK7USdFh0w3.

has been leaked to 2 third-party domains, owned by 1 different companies courtesy 11 website.

<table>
<thead>
<tr>
<th>Company</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td><a href="http://www.flixbus.de">www.flixbus.de</a></td>
</tr>
<tr>
<td>Facebook</td>
<td>shop.flixbus.de</td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.bild.de">www.bild.de</a></td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.trainline.eu">www.trainline.eu</a></td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.cleartrip.com">www.cleartrip.com</a></td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.foodora.com">www.foodora.com</a></td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.foodora.de">www.foodora.de</a></td>
</tr>
<tr>
<td>Facebook</td>
<td>edition.cnn.com</td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.nytimes.com">www.nytimes.com</a></td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.c-and-a.com">www.c-and-a.com</a></td>
</tr>
<tr>
<td>Facebook</td>
<td><a href="http://www.macworld.com">www.macworld.com</a></td>
</tr>
</tbody>
</table>
Also found fr=0Sh6fFpK7USdFh0w3. in third-party urls courtesy www.trainline.eu:

https://www.facebook.com/tr/?id=1674453164124987&ev=PageView&dl=https://www.trainline.eu/order/4a83-

Cookie fr=0Sh6fFpK7USdFh0w3. Ba5J4E..Fsl.1.0.BbT7LM.

---

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>From</th>
<th>To</th>
<th>Train No</th>
<th>Class</th>
<th>Seat</th>
<th>Fare</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 AUG</td>
<td>09:47</td>
<td>München Hbf</td>
<td>Frankfurt HBF</td>
<td>09:47</td>
<td>1st</td>
<td>C 380</td>
<td>€ 55.40</td>
</tr>
<tr>
<td></td>
<td>13:40</td>
<td>Frankfurt HBF</td>
<td>Marburg (HBF)</td>
<td>13:40</td>
<td>1st</td>
<td>C 840</td>
<td>€ 56.40</td>
</tr>
<tr>
<td>5 AUG</td>
<td>13:56</td>
<td>Marburg (HBF)</td>
<td>München Hbf</td>
<td>13:56</td>
<td>1st</td>
<td>C 4160</td>
<td>€ 56.40</td>
</tr>
</tbody>
</table>

Your tickets have been sent to modi.konark@gmail.com

Wrong email address? Edit

€111.80

Ticket reference: [Redacted]

Proof of payment
Purchased on 07 July 2018

Refund and exchange: Sparenpreis

Invoice
LOCAL SHERIFF

Also found in third-party urls courtesy www.foodora.de:


Cookie f=0Sh6lfPfpK7UsdFh0w3...Ba5J4E..FuR.1.0.BbkTy8.
<table>
<thead>
<tr>
<th>URL</th>
<th>Cookie</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.bild.de">www.bild.de</a></td>
<td>fr=0Sh6fFpK7USdFh0w3.</td>
</tr>
<tr>
<td>edition.cnn.com</td>
<td>fr=0Sh6fFpK7USdFh0w3.</td>
</tr>
<tr>
<td><a href="http://www.trainline.eu/order/3e5">www.trainline.eu/order/3e5</a>&lt;Redacted&gt;</td>
<td>fr=0Sh6fFpK7USdFh0w3.</td>
</tr>
</tbody>
</table>

Analytics Backend
PLATFORMS

https://github.com/cliqz-oss/local-sheriff
https://github.com/cliqz-oss/local-sheriff#app-store-links
How to explain the problem to an average user?
Migraciones
VISUALIZAR'17
15-30 septiembre
$3 \omega \tau \nu^2 = \delta$

$\sqrt{0 - 2} = 2 \mu \iota \varepsilon$

$x^2 \eta y^2$
World known
(visited websites)

Underworld
(third parties involved)
Video demo not available on the PDF version.
The video is available at:
https://assets.trackula.org/2019-trackula-plugin-usage.mp4
Datos recopilados desde Dec 09 2018
Has visitado 24 sitios
Has conectado con otros 588 sitios de terceros

- www.eldiario.es
- www.idealista.com
- www.infojobs.net
- www.booking.com
- www.milanuncios.com
FUTURE WORK

- Local Sheriff: notify user of form data leaked
- Local Sheriff as a privacy analysis “engine”
- Lower-level language (wasm); HAR support
- Trackula as a UI and client of Local Sheriff
- Sharing technology for GDPR compliance
Questions?

Konark Modi | @konarkmodi
Santiago Saavedra | @ssice
Sofía Próspere | @sofipros

github.com/cliqz-oss/local-sheriff

trackula.org