Today's talk
Exodus Privacy at FOSDEM 2019

Who we are

• Guiness
• pnu

What we will talk about

• The behavior of mobile applications and its consequences for our privacy
• What Exodus Privacy tries to do against that
Who we are
Exodus Privacy

- Group of French hacktivists
- Non-profit organization founded in October 2017
- Undefined number of members
- Strict legal rules
- 2 main collaborations:
  - Yale Privacy Lab
  - F-Droid
- We do FLOSS
Our goal
Make people aware of permanent tracking on smartphones
How we do

- Develop the **exodus** privacy auditing platform
- Identify trackers by code signatures
- Statically analyze **APK** files

We develop a transparency tool allowing people to know what is embedded in Android applications.
METEO FRANCE

Version: 6.1.5
Creator: Météo-France
Downloads: 5,000,000+ downloads

This report was automatically issued on Jan. 10, 2019, 11:43 p.m..
This report was automatically updated on Jan. 10, 2019, 11:43 p.m.

We have found code signature of the following trackers in the application:
- AdColony
- Amazon Advertisement
- AppLovin
- ATInternet
- Facebook Ads
- Facebook Analytics
- Facebook Login
- Facebook Share
- Flurry
- Google Ads
- Google Analytics
- Google CrashLytics
- Google DoubleClick
- Google Firebase Analytics
- Google Maps
- Google Play Services
- Google Play Store
- LinkedIn
- Localytics
- Mixpanel
- Open Mobile
- OpenGL
- OpenWRT
- Oracle
- PayPal
- Picasa
- Platform ONE
- Pratik
- Quelle
- RAVEN
- Rabbitmq
- Rival
- Salesforce
- Salesforce Mobile Analytics
- Salesforce Mobile SDK
- Sepia
- Shazam
- Skype
- Skype for Business
- Spire
- Stubhub
- Sumo
- Talkdesk
- Telefonica
- Travelfusion
- Uplight
- Upmob
- Verifone
- Vidyo
- WeChat
- Wi-Fi Information
- Yahoo
- Yandex
- YouCam
- Zenfone
- Zillow
- Zomato
- Zotero

Permissions

We have found the following permissions in the application:

- ACCESS_COARSE_LOCATION (android.permission)
  Access Approximate Location (Network-Based)
  Dangerous

- ACCESS_FINE_LOCATION (android.permission)
  Access Precise Location (GPS And Network-Based)
  Dangerous

- ACCESS_NETWORK_STATE (android.permission)
  View Network Connections
  Normal

- ACCESS_WIFI_STATE (android.permission)
  View Wi-Fi Connections
  Normal

- CAMERA (android.permission)
  Take Pictures And Videos
  Dangerous

- INTERNET (android.permission)
  Have Full Network Access
  Normal

- RECEIVE_BOOT_COMPLETED (android.permission)
  Normal
What we call a tracker

“A tracker is a piece of software meant to collect data about you or your usages.”

Like Ogury, Google Analytics, Teemo, and many other.
Flurry

Go to the tracker web page.

Detection rules

- Code detection rule: com.flurry.
- Network detection rule: flurry\..com

Primary Location

United States

Website

https://developer.yahoo.com

About

Flurry is part of the Yahoo Developer network suite. Flurry's product, Flurry Analytics, offers mobile analytics, monetization, and advertising services Yahoo, 01; Yahoo, 14; Wikipedia, 01).

Ownership

Oath Inc. (subsidiary of Verizon Communications; Oath includes Yahoo and AOL) Wikipedia, 01; Ars Technica, 01

Products and Services

Flurry Analytics:

- Utilizes tracking to analyze user interaction, correlating with other users
- Groups and correlates user data

Available reports for this tracker

- Mobile Security: Antivirus, Wi-Fi VPN & Anti-Theft
  - 5.1.0.086
  - Jan. 30, 2019, 7:10 p.m.

- Seznam.cz
  - 6.1.0
  - Jan. 30, 2019, 1:26 p.m.

- WiFi Password Recovery
  - 2.5.5
  - Jan. 30, 2019, 1:07 p.m.

- Lyrics Mania - Music Player
  - 3.3.20
  - Jan. 30, 2019, 1:05 p.m.

- Musixmatch Lyrics
  - 7.2.7
  - Jan. 30, 2019, 1:05 p.m.

- Photo Editor Pro – Filters, Sticker, Collage Maker
  - 4.7.6
  - Jan. 30, 2019, 12:31 p.m.

- Edge Screen S9 Note 9
  - 1.7.6
  - Jan. 30, 2019, 12:02 p.m.

- Microsoft Outlook
  - 3.6.2
  - Jan. 30, 2019, 11:53 a.m.

- Deezer Music
  - 6.6.5.271
  - Jan. 30, 2019, 10:05 a.m.

- File Manager
  - 2.6.9
  - Jan. 30, 2019, 9:45 a.m.

- 4.5.1
  - Jan. 30, 2019, 9:31 a.m.
How we detect them

Static analysis

- List Java classes embedded in the APK
- Find classes matching the tracker code signature
- Gplaycli: download the APK and get application details from Google Play
- Androguard: get permissions, code version and certificates
- Dexdump: extract list of classes from APK file
Static analysis

1. APK file
2. unzip
3. dex files
4. dxdump
5. trackers signatures
6. Java classes
7. match
8. embedded trackers
Static analysis

dexdump classes*.dex | perl -n -e\'/[A-Z]+(?:\w+[/])\w+\}/ && print "$1\n" | sort | uniq

com/amazon/device/ads/UserIdParameter
com/amazon/device/ads/Version
com/amazon/device/ads/VideoActionHandler
com/amazon/device/ads/ViewabilityChecker
com/amazon/device/ads/ViewabilityCheckerFactory
com/amazon/device/ads/ViewabilityInfo
com/amazon/device/ads/ViewabilityJavascriptFetcher
com/amazon/device/ads/ViewabilityJavascriptFetcherListener
com/amazon/device/ads/ViewabilityObserver

match

com.amazon.device.ads.

Amazon Ads is embedded
Our tools
Inside Exodus web platform
Exodus Privacy Android Application

- Show the **trackers** and **required permissions** in the apps in your smartphone
- Available on F-Droid and Google Play!
Exodify: Exodus Privacy in your browser

- Browser extension for Firefox and Chrome
- Displays the number of trackers embedded in each application
- Quick link to submit the application for a new analysis
Exodify: Exodus Privacy in your browser

Applications

- Banque Caisse d'Epargne
- Ma Banque CREDIT AGRICOLE TEC
- L'Appli Société Générale Société Générale
- Banque pour tablette Caisse d'Epargne
- La Banque Postale
- Banque Populaire BANQUE POPULAIRE
- Carrefour Banque Carrefour Groupe
- N26 La Banque N26
- Banque Populaire BANQUE POPULAIRE
- Bankin, l'app n°1
- AXA Banque
- Mes Comptes BNP
- BANQUE CIC
- BNP PARIBAS
- Orange
- LCI
- CIS
- DCG
What about developers?

exodus-standalone

- exodus CLI client for local APK static analysis
- Can be used by developers to scan their own app before release
- Prints reports as simple text or JSON
First results
What we did during the last past year

• We effectively exist since 24/11/2017 - first public release

• We have identified 152 trackers and analyzed +48000 applications

• We helped developers and companies like Qwant to clean their applications

• We provided a lot of advice and courses to developers who want to respect privacy

• We did deep audits of several applications like Baby+

• We provided statistics and data sets to journalists and labs

• We opened a REST API

• We created 3 animation videos to explain trackers to the public

Everything is free and open 🎄
## Most frequent trackers

<table>
<thead>
<tr>
<th>Tracker</th>
<th>In How Many Apps</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Firebase Analytics</td>
<td>24546 apps</td>
<td>50%</td>
</tr>
<tr>
<td>Google Ads</td>
<td>24189 apps</td>
<td>50%</td>
</tr>
<tr>
<td>Google DoubleClick</td>
<td>20764 apps</td>
<td>42%</td>
</tr>
<tr>
<td>Google Analytics</td>
<td>18081 apps</td>
<td>37%</td>
</tr>
<tr>
<td>Google Crashlytics</td>
<td>17051 apps</td>
<td>35%</td>
</tr>
<tr>
<td>Facebook Login</td>
<td>12441 apps</td>
<td>25%</td>
</tr>
<tr>
<td>Facebook Share</td>
<td>11927 apps</td>
<td>24%</td>
</tr>
<tr>
<td>Facebook Analytics</td>
<td>11189 apps</td>
<td>23%</td>
</tr>
<tr>
<td>Flurry</td>
<td>8220 apps</td>
<td>16%</td>
</tr>
<tr>
<td>Facebook Ads</td>
<td>7644 apps</td>
<td>15%</td>
</tr>
<tr>
<td>Inmobi</td>
<td>7122 apps</td>
<td>14%</td>
</tr>
<tr>
<td>Facebook Places</td>
<td>6762 apps</td>
<td>13%</td>
</tr>
<tr>
<td>Twitter MoPub</td>
<td>4088 apps</td>
<td>8%</td>
</tr>
<tr>
<td>Unity3d Ads</td>
<td>3779 apps</td>
<td>7%</td>
</tr>
<tr>
<td>Moat</td>
<td>3670 apps</td>
<td>7%</td>
</tr>
<tr>
<td>AppsFlyer</td>
<td>3597 apps</td>
<td>7%</td>
</tr>
<tr>
<td>AppLovin</td>
<td>3000 apps</td>
<td>6%</td>
</tr>
<tr>
<td>Adjust</td>
<td>2329 apps</td>
<td>4%</td>
</tr>
<tr>
<td>AdColony</td>
<td>2228 apps</td>
<td>4%</td>
</tr>
<tr>
<td>HockeyApp</td>
<td>2207 apps</td>
<td>4%</td>
</tr>
<tr>
<td>Millennial Media</td>
<td>2206 apps</td>
<td>4%</td>
</tr>
</tbody>
</table>
**Baby+**

This application sends everything to Facebook: baby name, gender, feeds, type of feeds, ...

```plaintext
POST https://179.60.192.3/v2.5/579769162185818/activities?access_token=access_token&format=json&sdk=android HTTP/1.1
User-Agent: FBAAndroidSDK.4.10.0
Accept-Language: en_US
Content-Type: multipart/form-data; boundary=312ndDfv2rTHisIsAbouNdArYfORhtPEefj3q2f
Transfer-Encoding: chunked
Host: graph.facebook.com
Connection: Keep-Alive
Accept-Encoding: identity
```

with this payload

```json
format: json
sdk: android
custom_events_file: [{"_eventName":"User Info","_logTime":1513302840,"_ui":"unknown","Country":"US","Language":"en","Relationship ":"mother","Loggedin":"NO"},{"_eventName":"Child Info","_logTime":1513302840,"_ui":"unknown","Is Breast Feeding":"NO","BF Days Complete":0,"Child Name":"erewrwerwerwer","Child Gender":"boy"},{"_eventName":"Viewed Undefined","_logTime":1513302850,"_ui":"unknown","valueToSum":1},{"_eventName":"Viewed Feed","_logTime":1513302850,"_ui":"unknown","valueToSum":1}]
event: CUSTOM_APP_EVENTS
advertiser_id: 0ea76bd4-3a79-432d-9c0f-c6f6b3cf8e66
advertiser_tracking_enabled: true
installer_package: com.android.vending
anon_id: XZfa9bbd90-abel-4736-9abf-5966513a82eb
application_tracking_enabled: true
extinfo: ["a2","com.hp.babyapp",25,"1.6.1","6.0.1","VirtualBox","en_US","GMT+01:00","",768,976,"1.00",2,98,96]
application_package_name: com.hp.babyapp
```
We are in the press too

- **MotherBoard** - The Targets of Mobile Apps: Your Health, Your Ancestors, […]
- **Numerama** - Lutter contre les mouchards des apps, une cause citoyenne : […]
- **The Guardian** - Three quarters of Android apps track users with third party tools
- **BoingBoing** - Researchers craft Android app that reveals to find horrific […]
- **Le Monde** - Des mouchards cachés dans vos applications pour smartphones
- **Next Impact** - Rencontre avec Exodus Privacy, qui révèle les trackers […]
- **The Intercept** - Staggering Variety of Clandestine Trackers Found in Popular […]
- +8000 articles in +20 languages during the first 6 months
We are known by the CNIL

On Feb. 14th 2018 we met the people from "CNIL" (France Supervisory Authority) in their office in Paris.

Exchanges were very interesting from both sides and their interest is promising.

The CNIL will use exodus for preliminary investigations.
Even French TV knows about us

We made, for the French public TV channel *France2*, a TV report about Waze application and all the "unknown leaks" of GPS data.

The report was broadcast on Feb. 24th 2018.

The replay can be found on [Youtube](https://www.youtube.com).
Our material
Communication

We use different ways to make us visible:

• Stickers 😊
• Flyers
• Peertube and YouTube channel
• Mastodon, Twitter and Facebook accounts
• Conferences like today
Our future
What's next

- **Revamp the reports** to make them more readable and comprehensive
- Create more videos and podcasts to **explain tracking on mobile**
- Continue to animate a Facebook page, a Peertube and a Youtube channel
- Translate our media and tools into new languages
- **Gather more and more motivated people** to increase our volunteers number
- ...

What we need

We are a non-profit organization animated by volunteers. To stay alive, we need:

Help!
Contributions & Money

Q/A