Exodus Privacy - FOSDEM 2019

Today's talk

Exodus Privacy at FOSDEM 2019

Who we are

- Guiness
- pnu

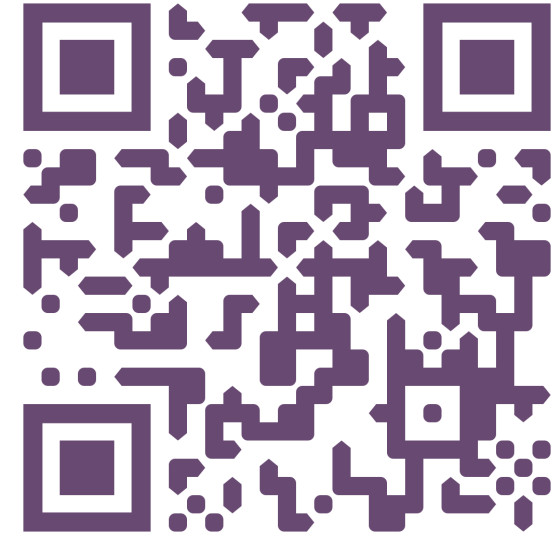
What we will talk about

- 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 **εxodus** 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.

9

22
trackers

13
permissions

METEO FRANCE

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

Other versions | On Google Play | APK fingerprint

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.**.

Signed by:

Fingerprint: `97450e0bcd3a5b0f016c6d06d4d9e72b176cfcb9`
Issuer: `localityName=Lyon`
Subject: `localityName=Lyon`
Serial: `1303805585`

22 Trackers

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

13 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)`	

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

8220 Available reports for this tracker

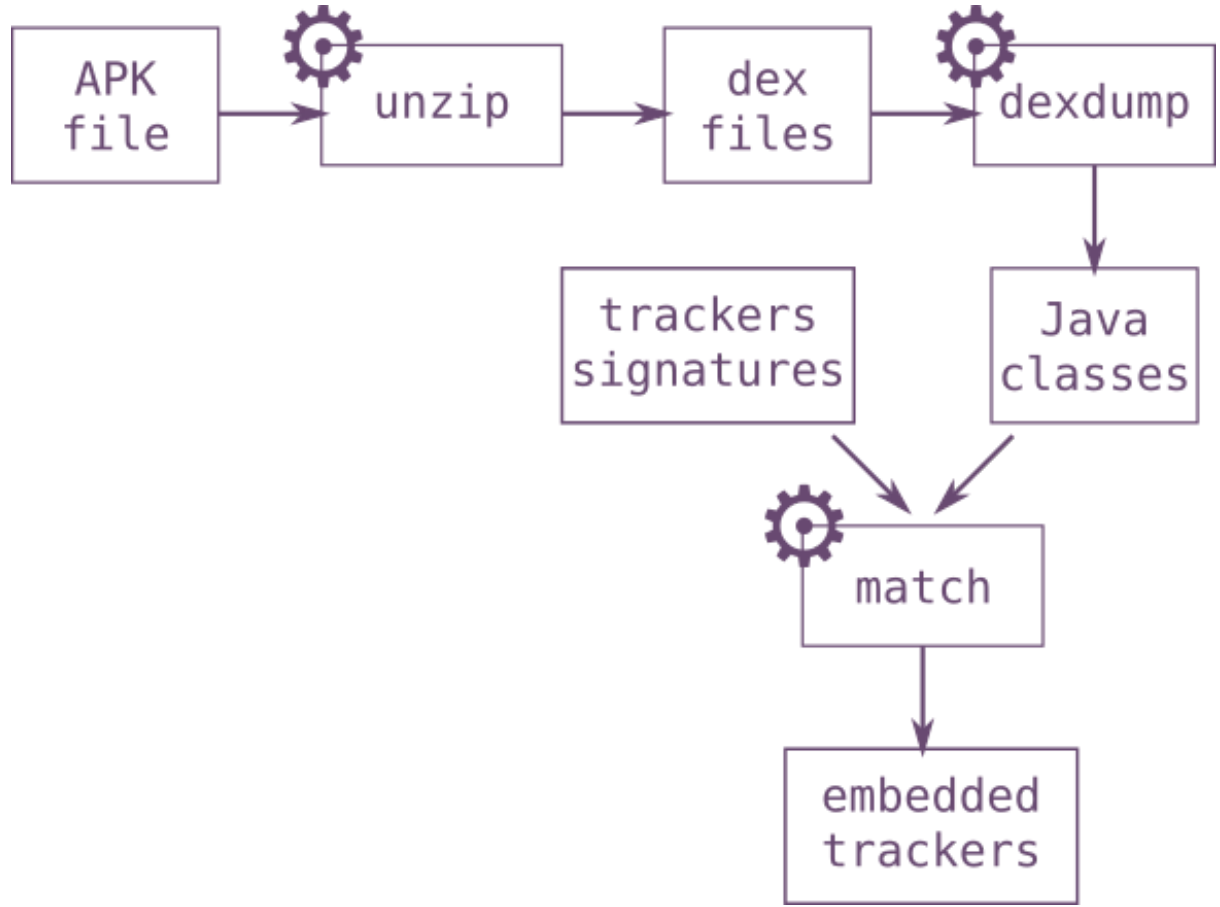
Mobile Security: Antivirus, Wi-Fi VPN & Anti-Theft	5.1.0.686	Jan. 30, 2019, 7:10 p.m.
Seznam.cz	6.1.0	Jan. 30, 2019, 1:26 p.m.
WiFi Password Recovery	2.5.5	Jan. 30, 2019, 1:07 p.m.
Lyrics Mania - Music Player	3.3.20	Jan. 30, 2019, 1:05 p.m.
Musixmatch Lyrics	7.2.7	Jan. 30, 2019, 1:05 p.m.
Photo Editor 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	3.0.2	Jan. 30, 2019, 11:53 a.m.
Deezer Music	6.0.5.271	Jan. 30, 2019, 10:05 a.m.
File Manager	2.0.9	Jan. 30, 2019, 9:45 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



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
```

Our tools

Inside εxodus web platform

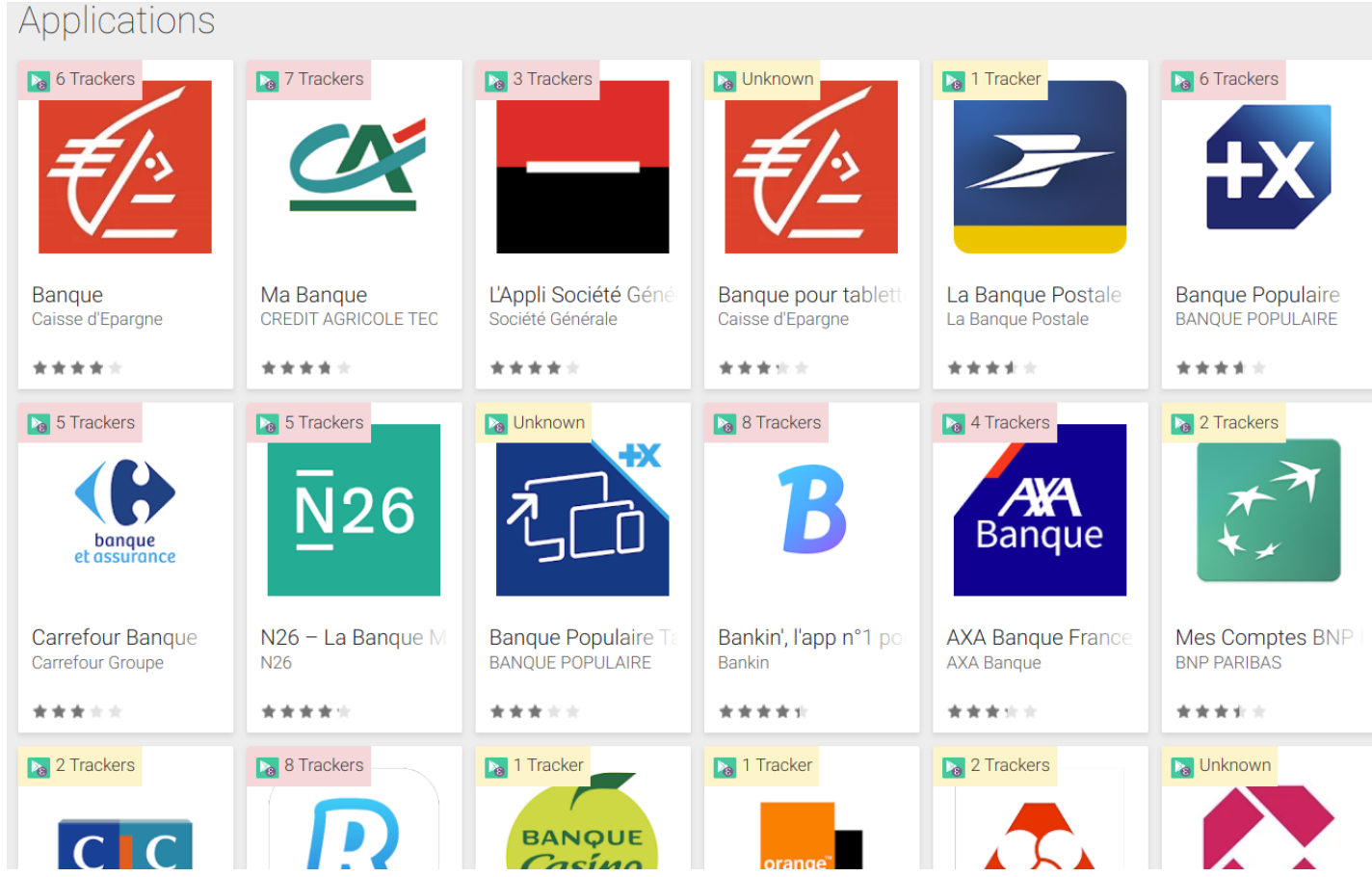
Exodus Privacy Android Application

- 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



What about developers?

exodus-standalone

- εxodus 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

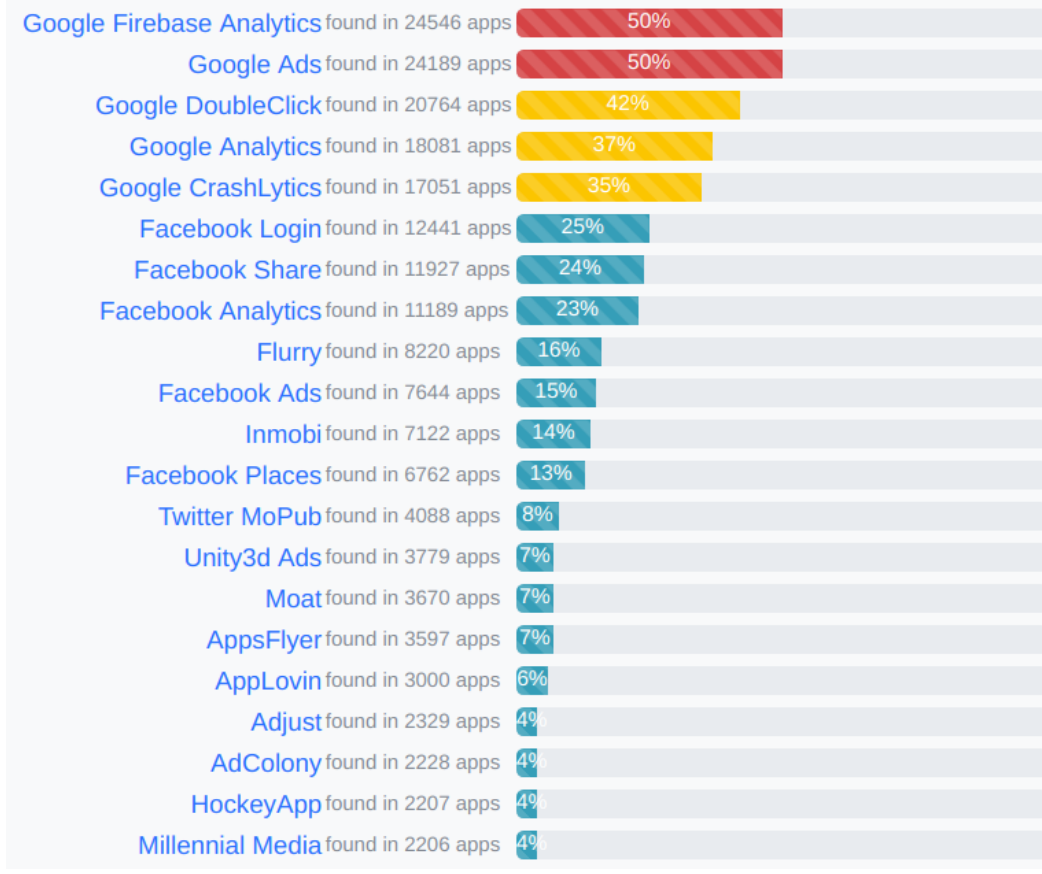
First results

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



Baby+

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

```
POST https://179.60.192.3/v2.5/579769162185818/activities?access_token=&format=json&sdk=android HTTP/1.1
User-Agent:    FBAndroidSDK.4.10.0
Accept-Language:    en_US
Content-Type:    multipart/form-data; boundary=3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
Transfer-Encoding:    chunked
Host:    graph.facebook.com
Connection:    Keep-Alive
Accept-Encoding:    identity
```

with this payload

```
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-abe1-4736-9abf-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 Inpact** - 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 εxodus for preliminary investigations.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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.

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

https://exodus-privacy.eu.org/en/page/contribute/

Q/A