Tracking Mobile Trackers

A Yale Privacy Lab Tech Primer

Share: privacylab.yale.edu/tmt

@YalePrivacyLab | privacylab@mastodon.social

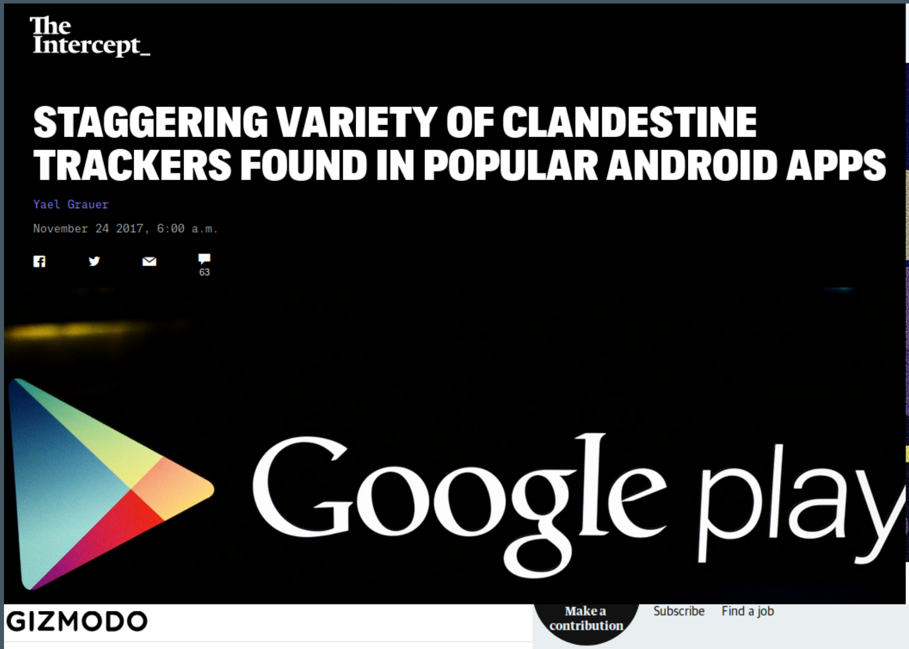
Presented by Sean O'Brien

Are you worried that your phone is listening to you?

That it is tracking your movements?

You are being tracked by your phone in some way. This primer will help explain and offer some solutions.

Our phones are full of naughty apps.

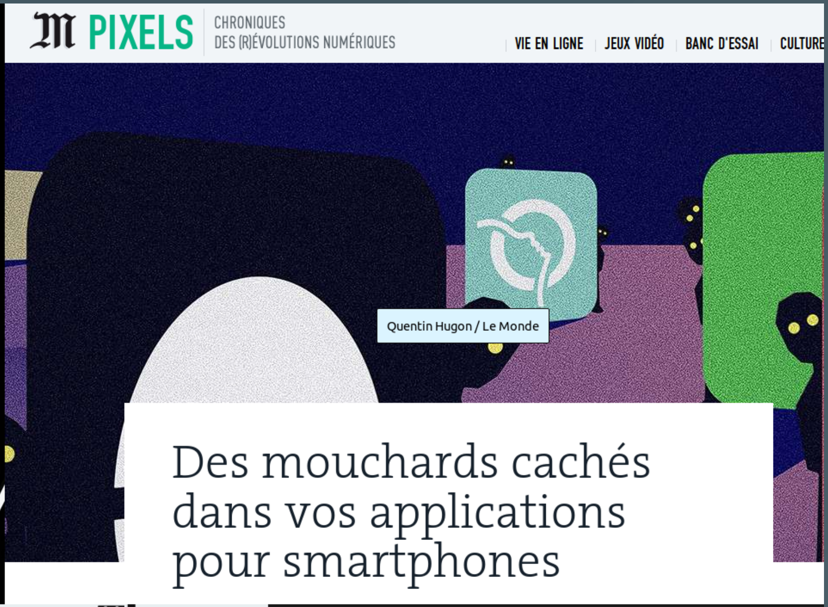

The Intercept_

STAGGERING VARIETY OF CLANDESTINE TRACKERS FOUND IN POPULAR ANDROID APPS

Yael Grauer

November 24 2017, 6:00 a.m.

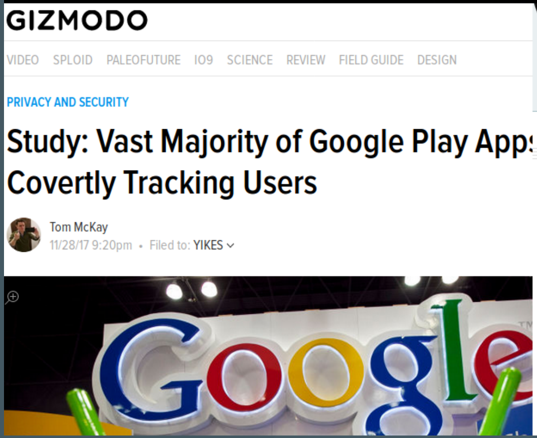
63


M PIXELS CHRONIQUES DES (R)ÉVOLUTIONS NUMÉRIQUES

VIE EN LIGNE | JEUX VIDÉO | BANC D'ESSAI | CULTURE

Quentin Hugon / Le Monde

Des mouchards cachés dans vos applications pour smartphones


GIZMODO

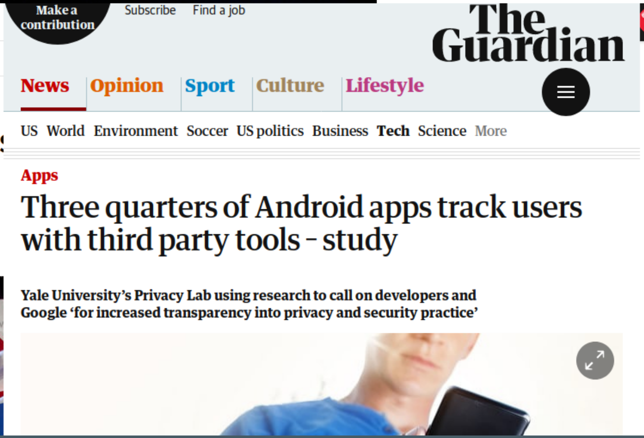
VIDEO SPLOID PALEOFUTURE IO9 SCIENCE REVIEW FIELD GUIDE DESIGN

PRIVACY AND SECURITY

Study: Vast Majority of Google Play Apps Covertly Tracking Users

Tom McKay

11/28/17 9:20pm • Filed to: YIKES


Make a contribution Subscribe Find a job

The Guardian

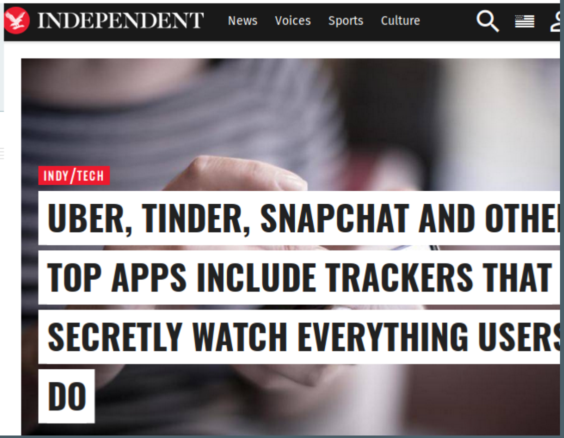
News Opinion Sport Culture Lifestyle

US World Environment Soccer US politics Business Tech Science More

Apps

Three quarters of Android apps track users with third party tools - study

Yale University's Privacy Lab using research to call on developers and Google 'for increased transparency into privacy and security practice'


INDEPENDENT News Voices Sports Culture

INDY/TECH

UBER, TINDER, SNAPCHAT AND OTHE

TOP APPS INCLUDE TRACKERS THAT

SECRETLY WATCH EVERYTHING USERS

DO

At Yale Privacy Lab, we help identify mobile trackers, code that runs inside apps without your knowledge or consent.

What Are Trackers?

- We use the term **trackers** broadly, to encompass traditional advertisement surveillance, analytics, behavioral and location tracking, as well as *developer tools* such as crash reporters.
- We're talking about trackers bundled for app developers as **Software Development Kits** (SDKs) though there are also other ways to track users.

We also focus on proximity and location tracking.

Trackers that use bluetooth and near-ultrasonic/ultrasonic signals are some of the worst offenders.

What About Apple?

We'll be talking about **Android apps in Google Play**.

Many of the same companies distributing Google Play apps **also distribute apps via Apple**, and tracker companies openly advertise SDKs compatible with multiple platforms.

Thus, advertising trackers may be concurrently packaged for Android **and iOS**, as well as more obscure mobile platforms.

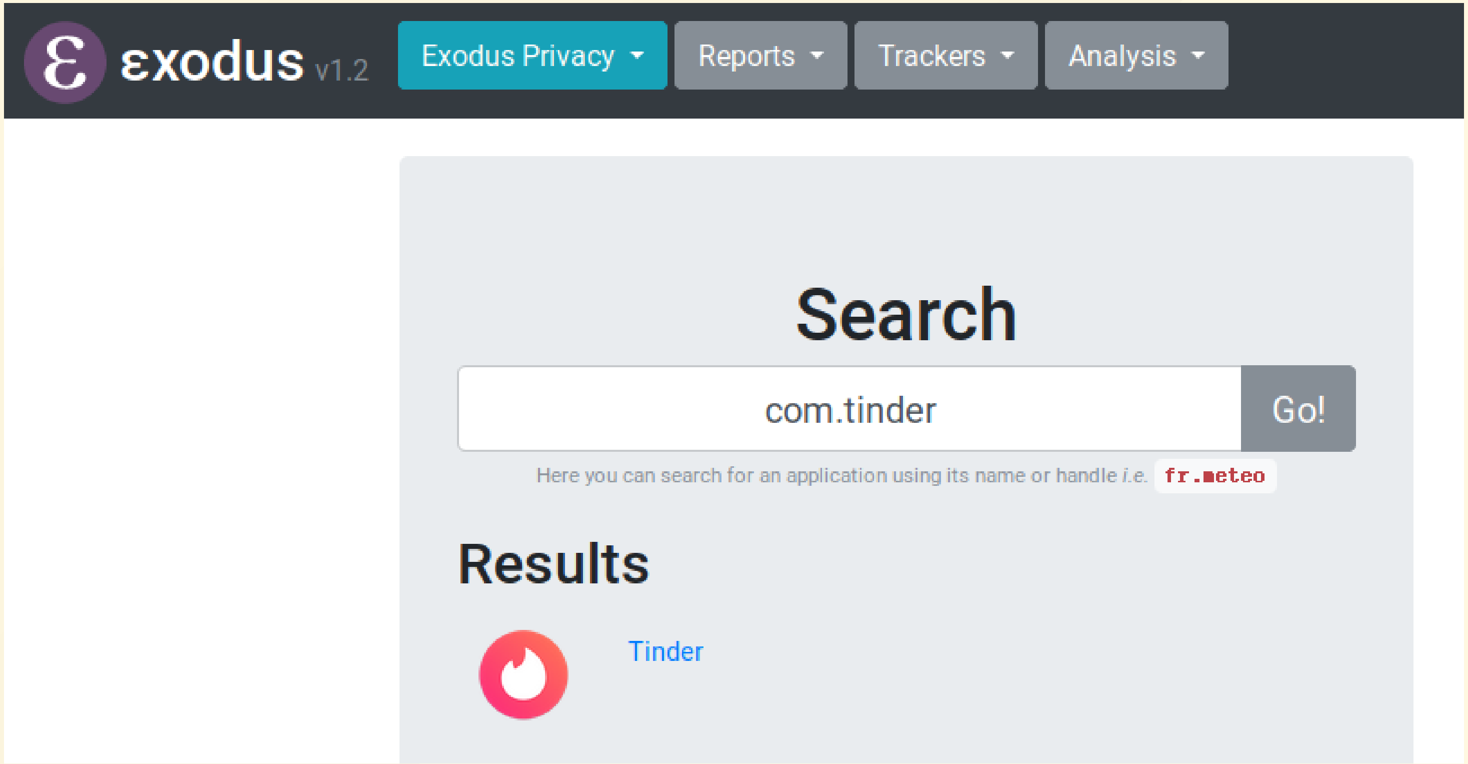
Digging Deep

- To really understand a specific app and privacy or security concerns, it takes **network analysis**.
- **App permissions** are a big indicator something might be amiss (RECORD_AUDIO etc.)

Be careful accepting permissions when you install an app!

We'll show you an easy way to detect tracker SDKs without needing to know anything about code, via the εxodus platform.

reports.exodus-privacy.eu.org



Search

com.tinder

Here you can search for an application using its name or handle *i.e.* `fr.meteo`

Results

Tinder

εxodus scans Android apps in Google Play.

Anyone can scan an app via a slick Web UI

Detecting Tracker SDKs

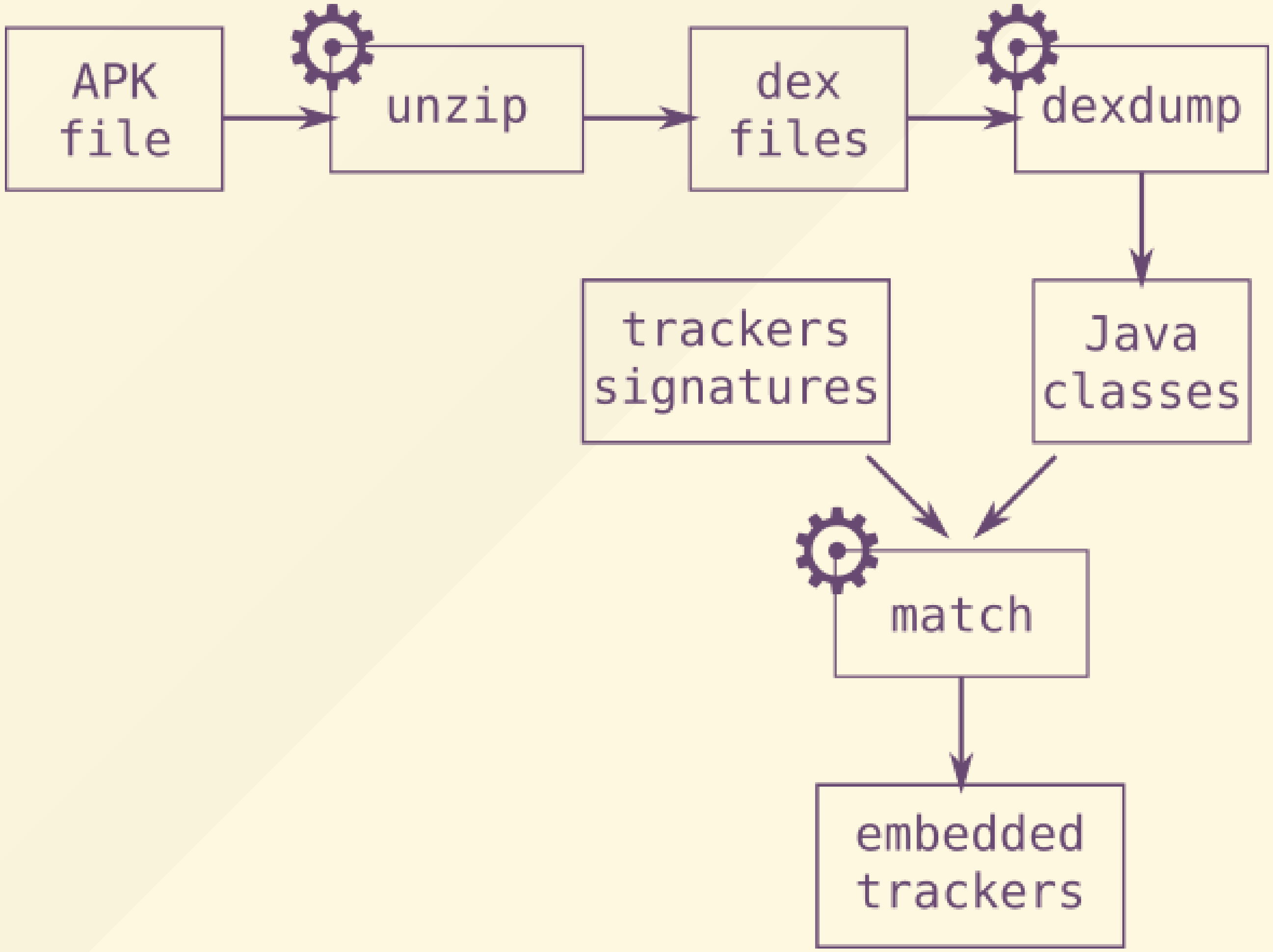
- εxodus scanner does **static analysis** of Android APKs to find signatures in embedded classes.
- Without εxodus, you can make educated guesses by looking at the **Android manifest** XML and classes* **DEX** files.
- Remember, there are legal restrictions on static analysis of iOS apps, but many of these apps also have trackers (more on that later).

Cory Doctorow on the subject:

“iOS is DRM-locked and **it's a felony** – punishable by a 5-year prison sentence and a $500,000 fine for a first offense in the USA under DMCA 1201, and similar provisions of Article 6 of the EUCD in France where Exodus is located – to distribute tools that bypass this DRM, even for the essential work of discovering whether billions of people are at risk due to covert spying from the platform.

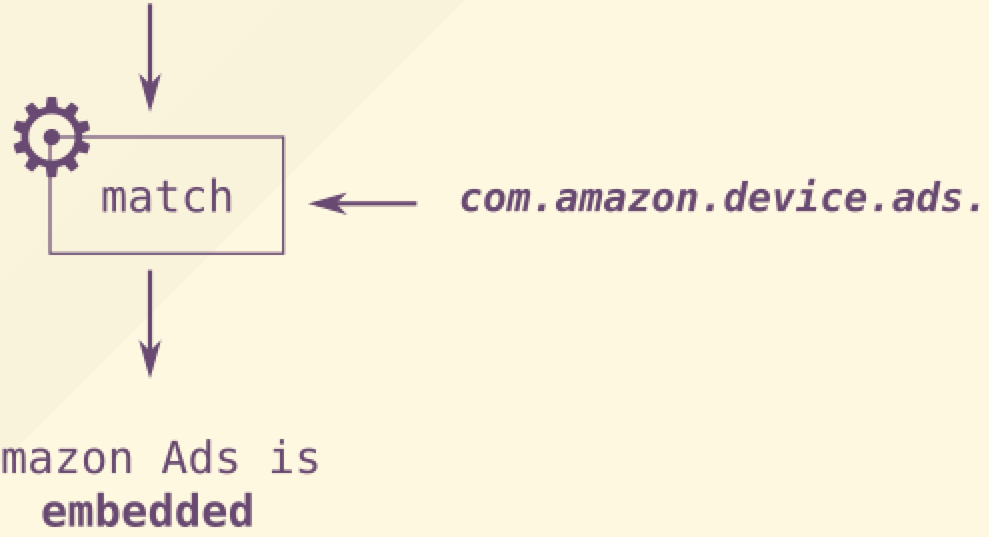
It's true that the US Copyright Office gave us a soon-to-expire exemption to this rule that started in 2016, but that exemption only allows Exodus to use that tool; **it doesn't allow Exodus to make that tool, or to distribute it so independent researchers can investigate iOS**.”

εxodus 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
```



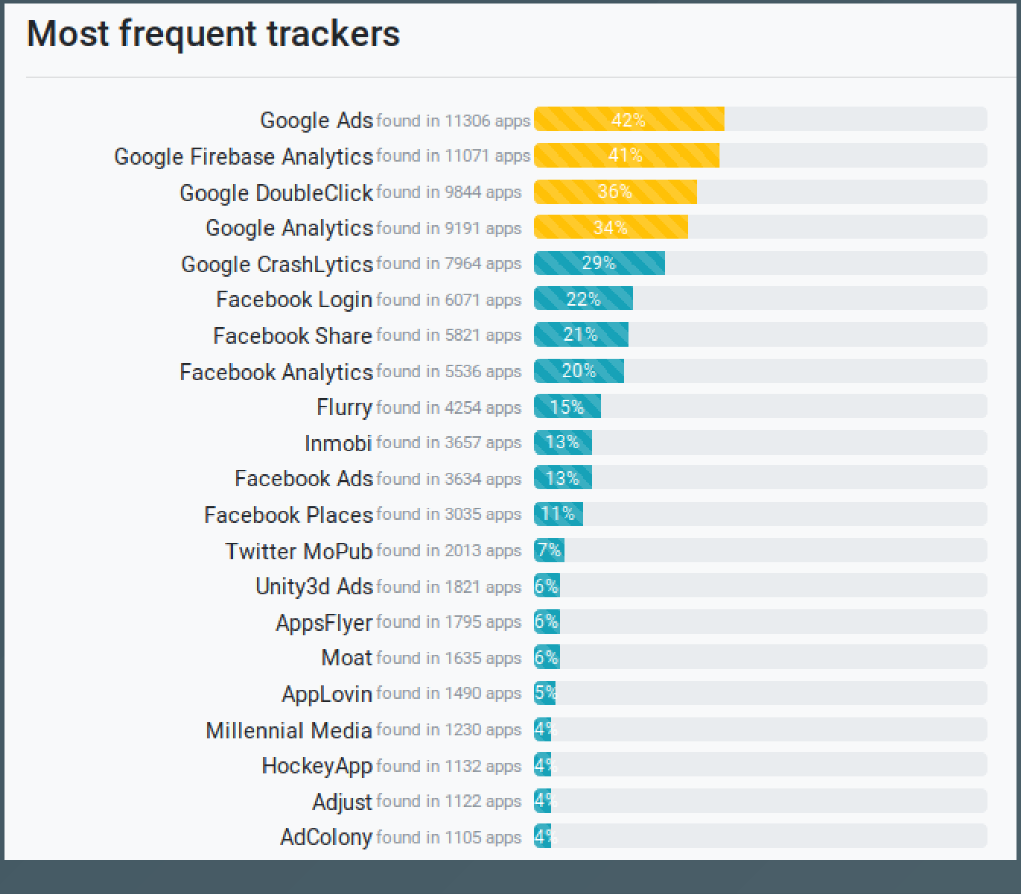
match

com.amazon.device.ads.

Amazon Ads is
embedded

Quick εxodus Stats

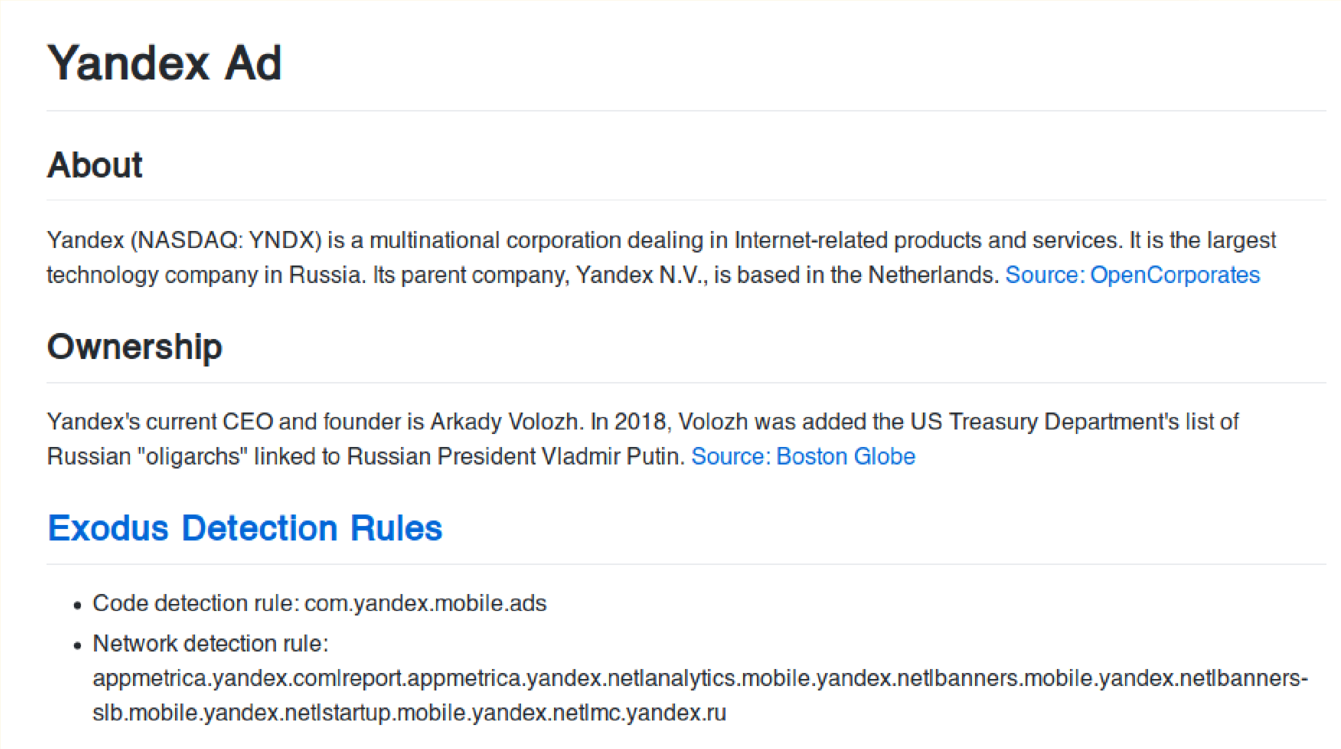
- 152 tracker signatures, 28,600 reports (Oct 1, 2018)
- 26,133 apps scanned, 400GB+ APK packages



Most frequent trackers

Google Ads	found in 11306 apps	42%
Google Firebase Analytics	found in 11071 apps	41%
Google DoubleClick	found in 9844 apps	36%
Google Analytics	found in 9191 apps	34%
Google CrashLytics	found in 7964 apps	29%
Facebook Login	found in 6071 apps	22%
Facebook Share	found in 5821 apps	21%
Facebook Analytics	found in 5536 apps	20%
Flurry	found in 4254 apps	15%
Inmobi	found in 3657 apps	13%
Facebook Ads	found in 3634 apps	13%
Facebook Places	found in 3035 apps	11%
Twitter MoPub	found in 2013 apps	7%
Unity3d Ads	found in 1821 apps	6%
AppsFlyer	found in 1795 apps	6%
Moat	found in 1635 apps	6%
AppLovin	found in 1490 apps	5%
Millennial Media	found in 1230 apps	4%
HockeyApp	found in 1132 apps	4%
Adjust	found in 1122 apps	4%
AdColony	found in 1105 apps	4%

Tracker Profiles



Yandex Ad

About

Yandex (NASDAQ: YNDX) is a multinational corporation dealing in Internet-related products and services. It is the largest technology company in Russia. Its parent company, Yandex N.V., is based in the Netherlands. Source: OpenCorporates

Ownership

Yandex's current CEO and founder is Arkady Volozh. In 2018, Volozh was added the US Treasury Department's list of Russian "oligarchs" linked to Russian President Vladmir Putin. Source: Boston Globe

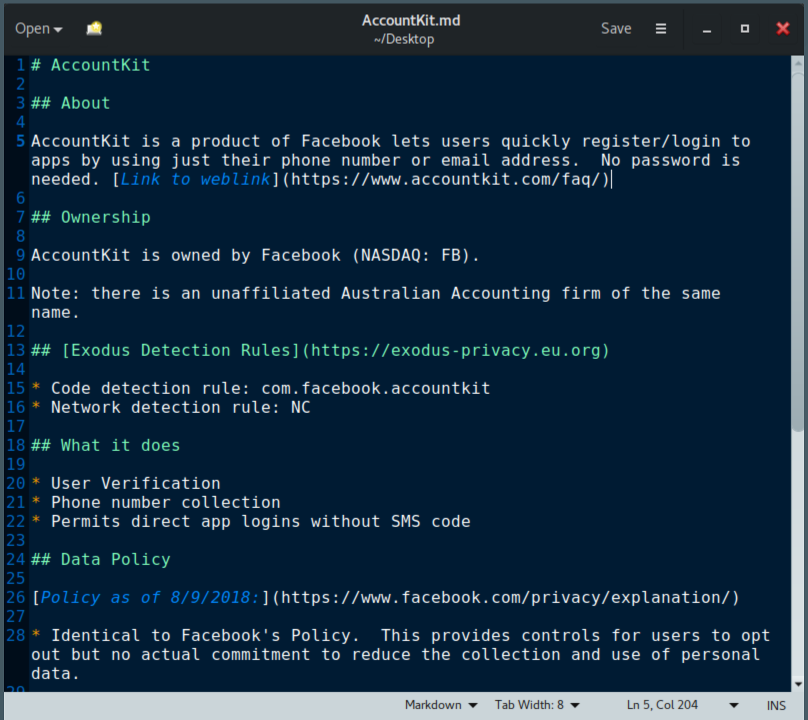
Exodus Detection Rules

- Code detection rule: com.yandex.mobile.ads
- Network detection rule: appmetrica.yandex.com|report.appmetrica.yandex.net|analytics.mobile.yandex.net|banners.mobile.yandex.net|banners-slb.mobile.yandex.net|startup.mobile.yandex.net|mc.yandex.ru

github.com/YalePrivacyLab/tracker-profiles

Calling crash reporters like HockeyApp, Crashlytics "trackers" has been controversial, though they have advanced analytics features/options.

Adding & Improving Tracker Profiles



```markdown
# AccountKit

## About

AccountKit is a product of Facebook lets users quickly register/login to
apps by using just their phone number or email address.  No password is
needed. [Link to weblink](https://www.accountkit.com/faq/)

## Ownership

AccountKit is owned by Facebook (NASDAQ: FB).

Note: there is an unaffiliated Australian Accounting firm of the same
name.

## [Exodus Detection Rules](https://exodus-privacy.eu.org)

* Code detection rule: com.facebook.accountkit
* Network detection rule: NC

## What it does

* User Verification
* Phone number collection
* Permits direct app logins without SMS code

## Data Policy

[Policy as of 8/9/2018:](https://www.facebook.com/privacy/explanation/)

* Identical to Facebook's Policy.  This provides controls for users to opt
out but no actual commitment to reduce the collection and use of personal
data.
```

- We are updating profiles, adding new ones.
- We're correlating companies via OpenCorporates.

We're looking for more contributors, and you can help us by contacting Yale Privacy Lab directly or finding us on github.

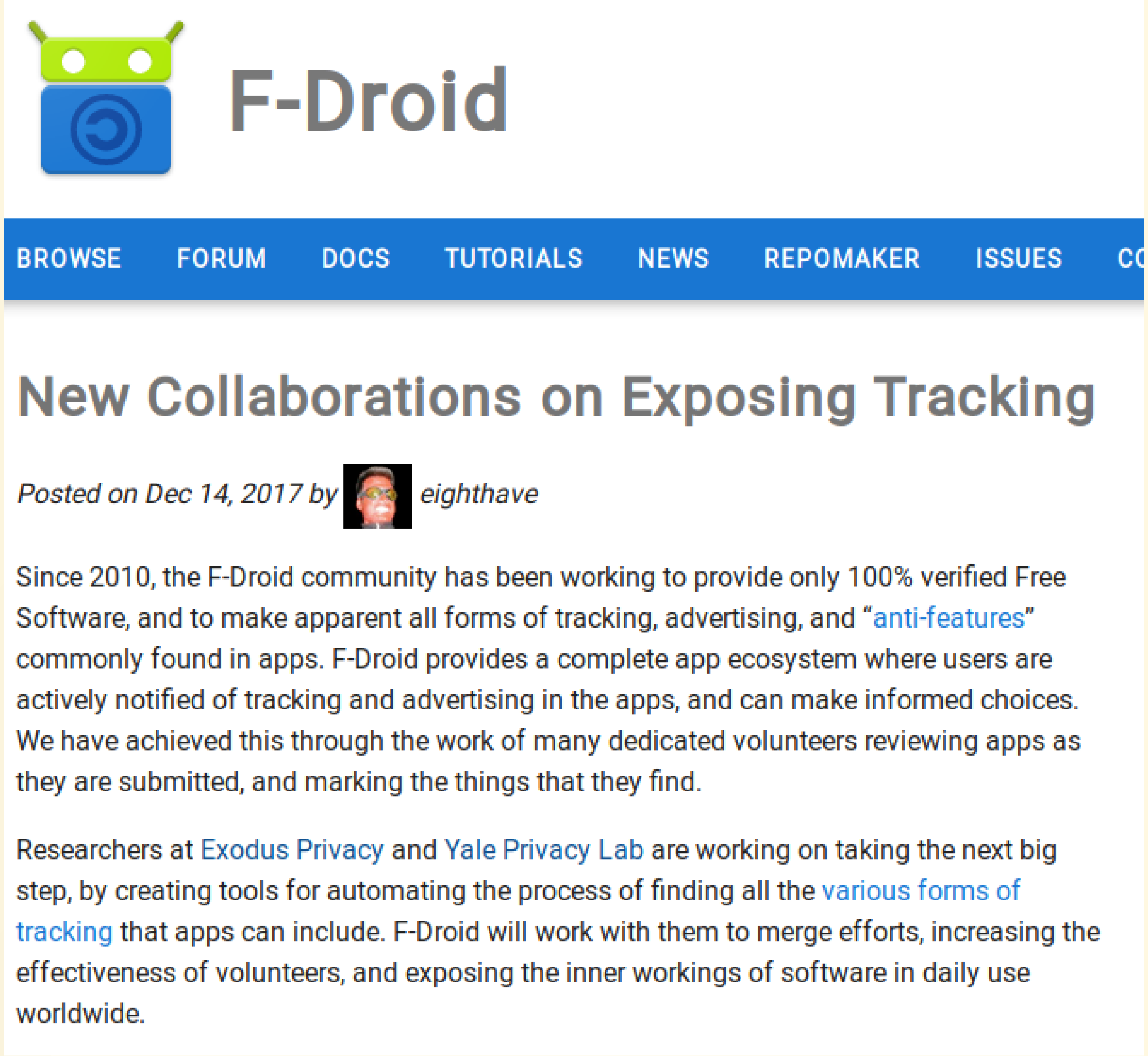
Mozilla has been guiding us via the Open Leaders Program and our mentor Josefina Caro Magaña of Beyond Activismo.

Real-World Impact:

Working on tracker profiles with us means you're contributing to software projects that protect privacy such as εxodus, F-Droid, Yalp Store, and our ultrasonic jammer apps.

Our tracker profiles go upstream to these software projects. Here are some examples.

F-Droid Collaboration



New Collaborations on Exposing Tracking

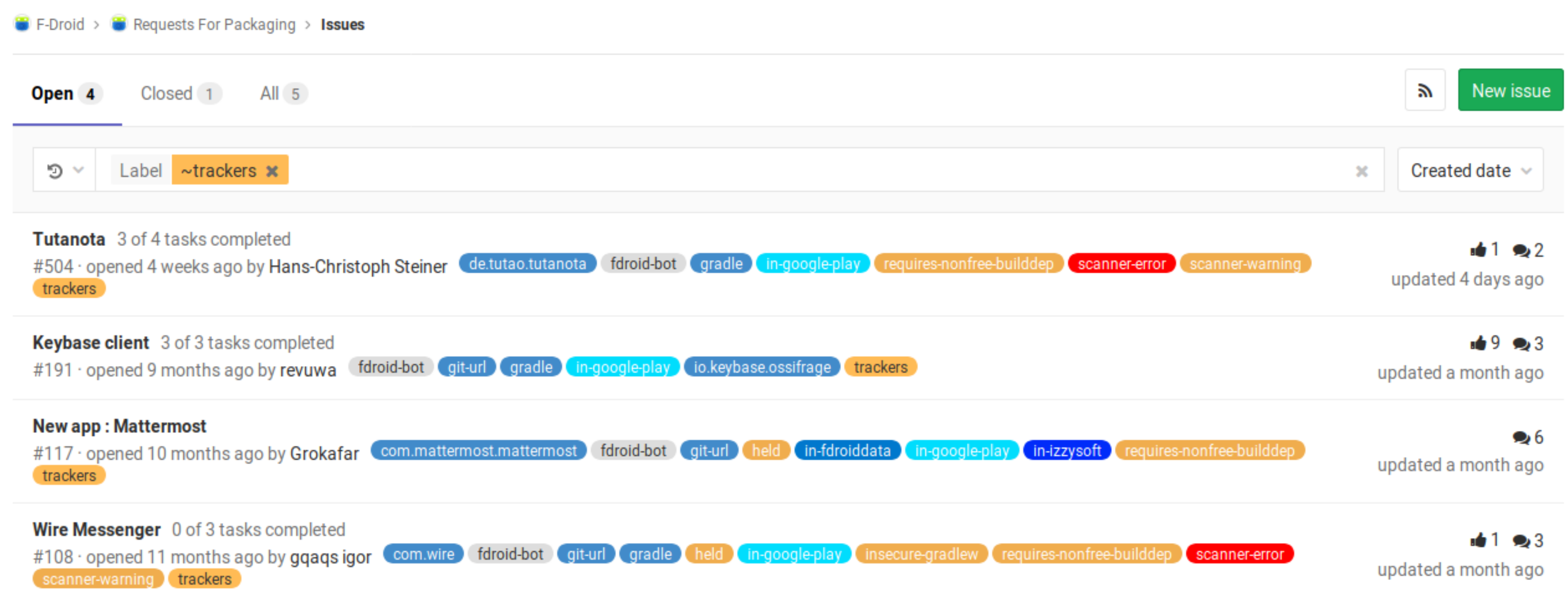
Posted on Dec 14, 2017 by eighthave

Since 2010, the F-Droid community has been working to provide only 100% verified Free Software, and to make apparent all forms of tracking, advertising, and “anti-features” commonly found in apps. F-Droid provides a complete app ecosystem where users are actively notified of tracking and advertising in the apps, and can make informed choices. We have achieved this through the work of many dedicated volunteers reviewing apps as they are submitted, and marking the things that they find.

Researchers at Exodus Privacy and Yale Privacy Lab are working on taking the next big step, by creating tools for automating the process of finding all the various forms of tracking that apps can include. F-Droid will work with them to merge efforts, increasing the effectiveness of volunteers, and exposing the inner workings of software in daily use worldwide.

F-Droid Blog Dec 2017

F-Droid Package Scanning



Tutanota 3 of 4 tasks completed
#504 · opened 4 weeks ago by Hans-Christoph Steiner de.tutao.tutanota fdroid-bot gradle in-google-play requires-nonfree-builddep scanner-error scanner-warning trackers
1 2
updated 4 days ago

Keybase client 3 of 3 tasks completed
#191 · opened 9 months ago by revuwa fdroid-bot git-url gradle in-google-play io.keybase.ossifrage trackers
9 3
updated a month ago

New app : Mattermost
#117 · opened 10 months ago by Grokafar com.mattermost.mattermost fdroid-bot git-url held in-fdroiddata in-google-play in-izzysoft requires-nonfree-builddep trackers
6
updated a month ago

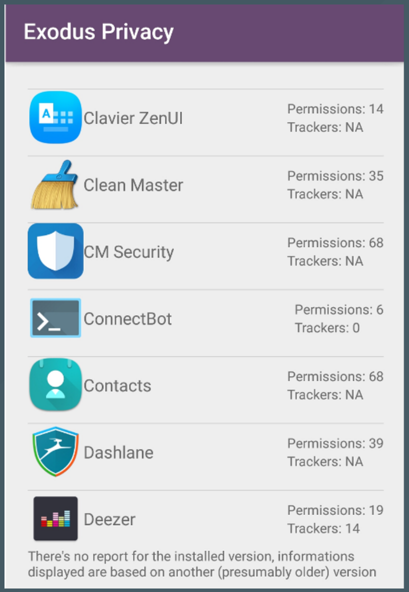
Wire Messenger 0 of 3 tasks completed
#108 · opened 11 months ago by gqaqs igor com.wire fdroid-bot git-url gradle held in-google-play insecure-gradlew requires-nonfree-builddep scanner-error scanner-warning trackers
1 3
updated a month ago

- AI/machine learning in the future?
- LibScout

https://gitlab.com/fdroid/rfp/issues?label_name[]=trackers

Free Software Projects

- Utilize εxodus API:
  - εxodus CLI
  - εxodus Android app
  - εxodify browser addons
- PilferShush Android app
- PiRanhaLysis network interception/analysis (PiRogue, PiPrecious, Phorcys)



Exodus Privacy

Clavier ZenUI — Permissions: 14 Trackers: NA

Clean Master — Permissions: 35 Trackers: NA

CM Security — Permissions: 68 Trackers: NA

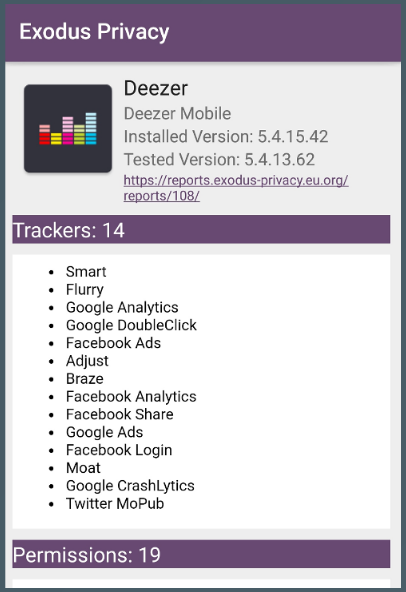
ConnectBot — Permissions: 6 Trackers: 0

Contacts — Permissions: 68 Trackers: NA

Dashlane — Permissions: 39 Trackers: NA

Deezer — Permissions: 19 Trackers: 14

There's no report for the installed version, informations displayed are based on another (presumably older) version



Exodus Privacy

Deezer
Deezer Mobile
Installed Version: 5.4.15.42
Tested Version: 5.4.13.62
https://reports.exodus-privacy.eu.org/reports/108/

Trackers: 14

- Smart
- Flurry
- Google Analytics
- Google DoubleClick
- Facebook Ads
- Adjust
- Braze
- Facebook Analytics
- Facebook Share
- Google Ads
- Facebook Login
- Moat
- Google CrashLytics
- Twitter MoPub

Permissions: 19

Now that we understand static analysis and tracker SDKs, let's talk about physical methods that companies use to track us.

Proximity Targeting

- Retailers are using **bluetooth** alongside **sonic** (near-ultrasonic/ultrasonic, 18kHz to 22kHz range) technology to track precise physical movements via **beacons**.
- The *de facto* bluetooth beacon standard is **Apple iBeacon**, one of the first to market.

Signatures of sonic tracker SDKs SilverPush, Alphonso, Lisnr, Shopkick, Fidzup, and Signal360 can be detected by εxodus. Their profiles are in our github repository.

We're detecting new trackers that utilize these creepy methods often. The latest is CopSonic.

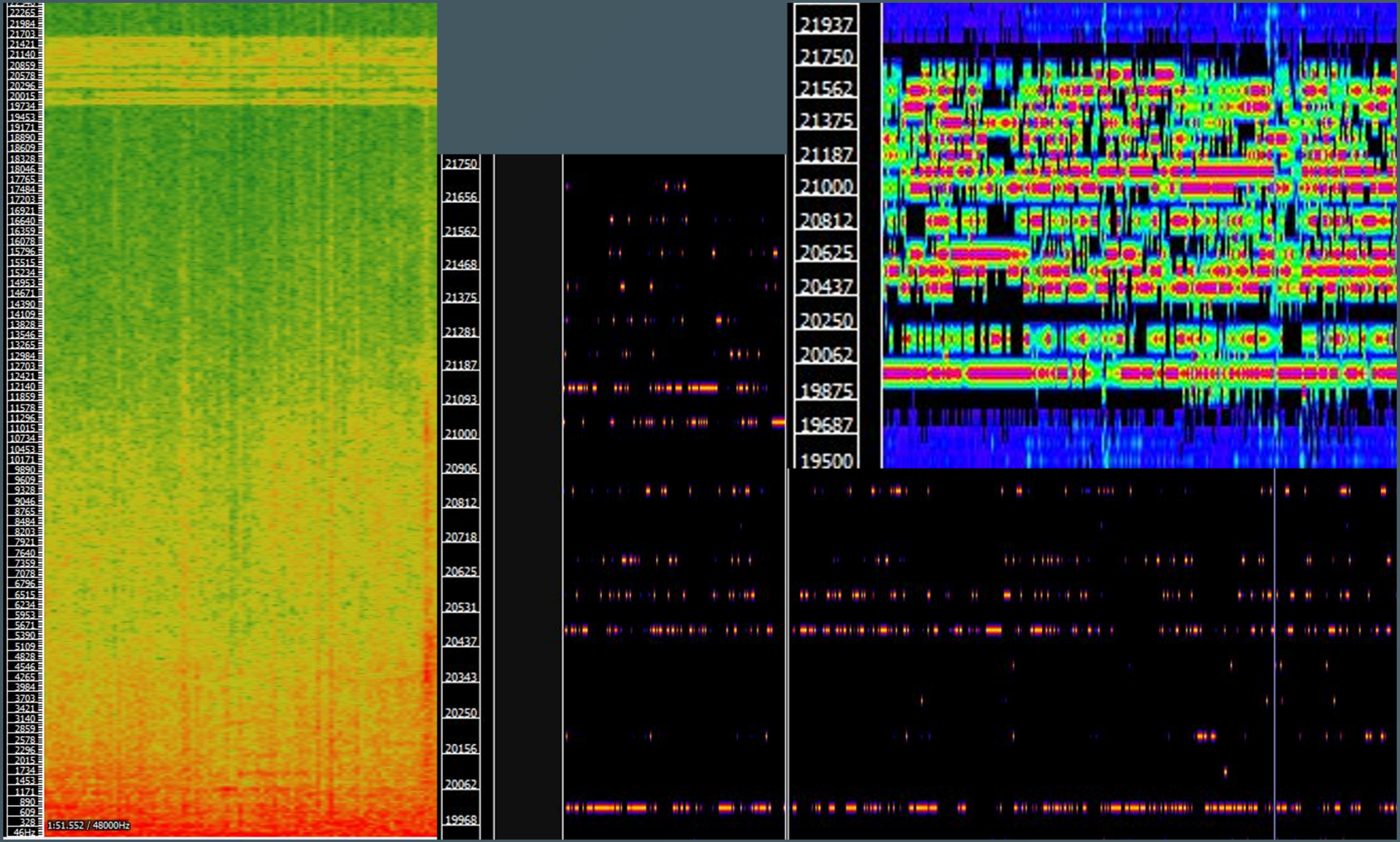
Example Beacon Devices

Source: https://en.wikipedia.org/wiki/IBeacon

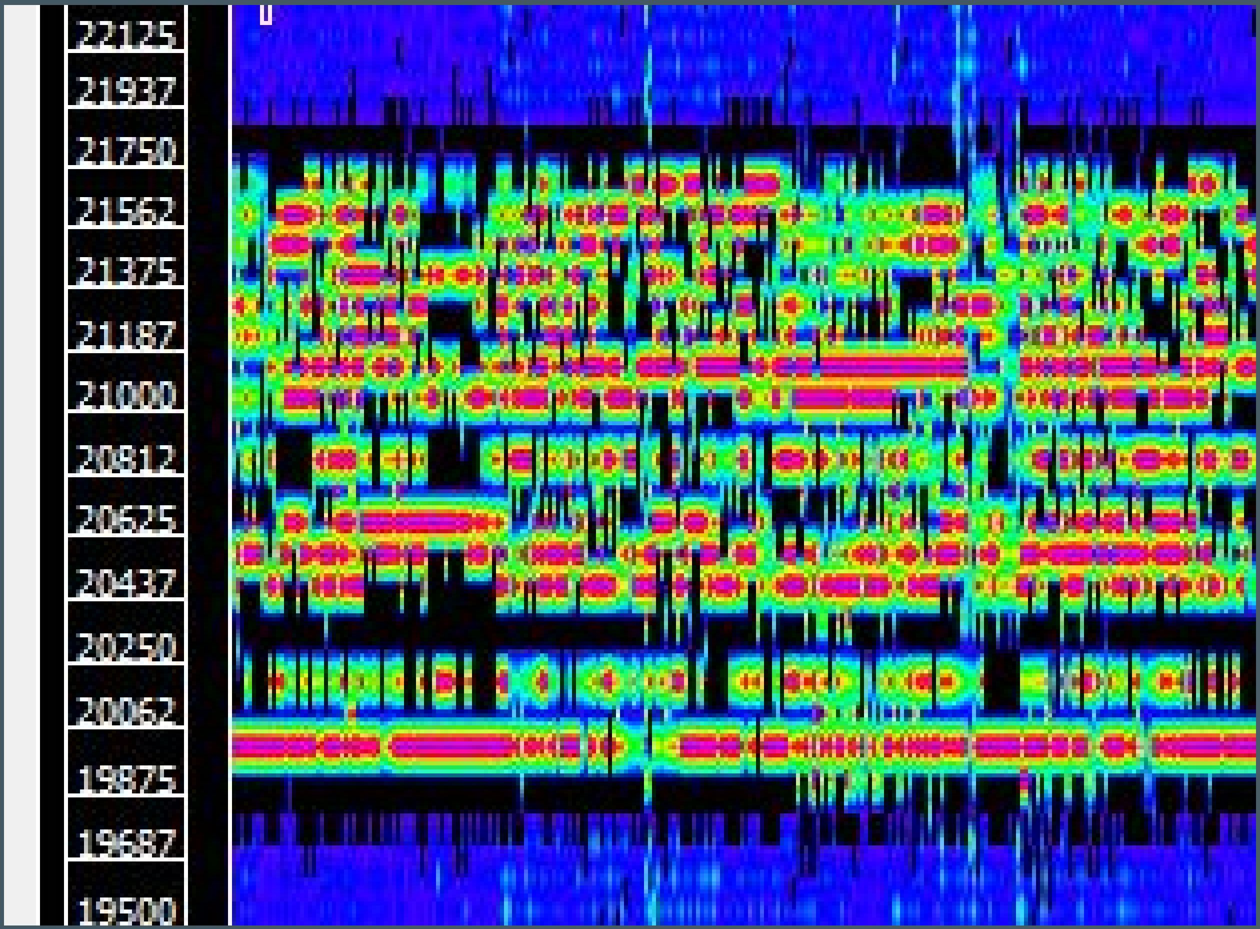
Important Caveats

- Beacons use a *combination* of technologies and **may not require an SDK** on a target person's phone.
- Special beacon devices are not required. Sonic tracking can occur via **stadium/arena** (Lisnr, Signal360), **retail** (Shopkick, Fidzup), **TV** (Alphonso, SilverPush) speakers.

Example Sonic Tracking Signals



Sonic Tracking Signal: Closer Look



Audio Sample, Macy's

Much More Info from Cityfreqs

Sonic Tracking Is Not Sci-Fi

- Frequency Shift Keying is the primary method.
- Some sonic trackers are very basic (Fidzup), others are complex (Shopkick).
- FTC warnings were issued for app devs who were using SilverPush in 2016.
- Many Alphonso apps were pulled in December 2017 after a *NYTimes* story.

Researchers and journalists have shared their app lists/checksums with us. We've got lists of sonic tracking apps still in the wild.

If you are interested in learning more, we can share these and other details (copies of ultrasonic recordings etc.)

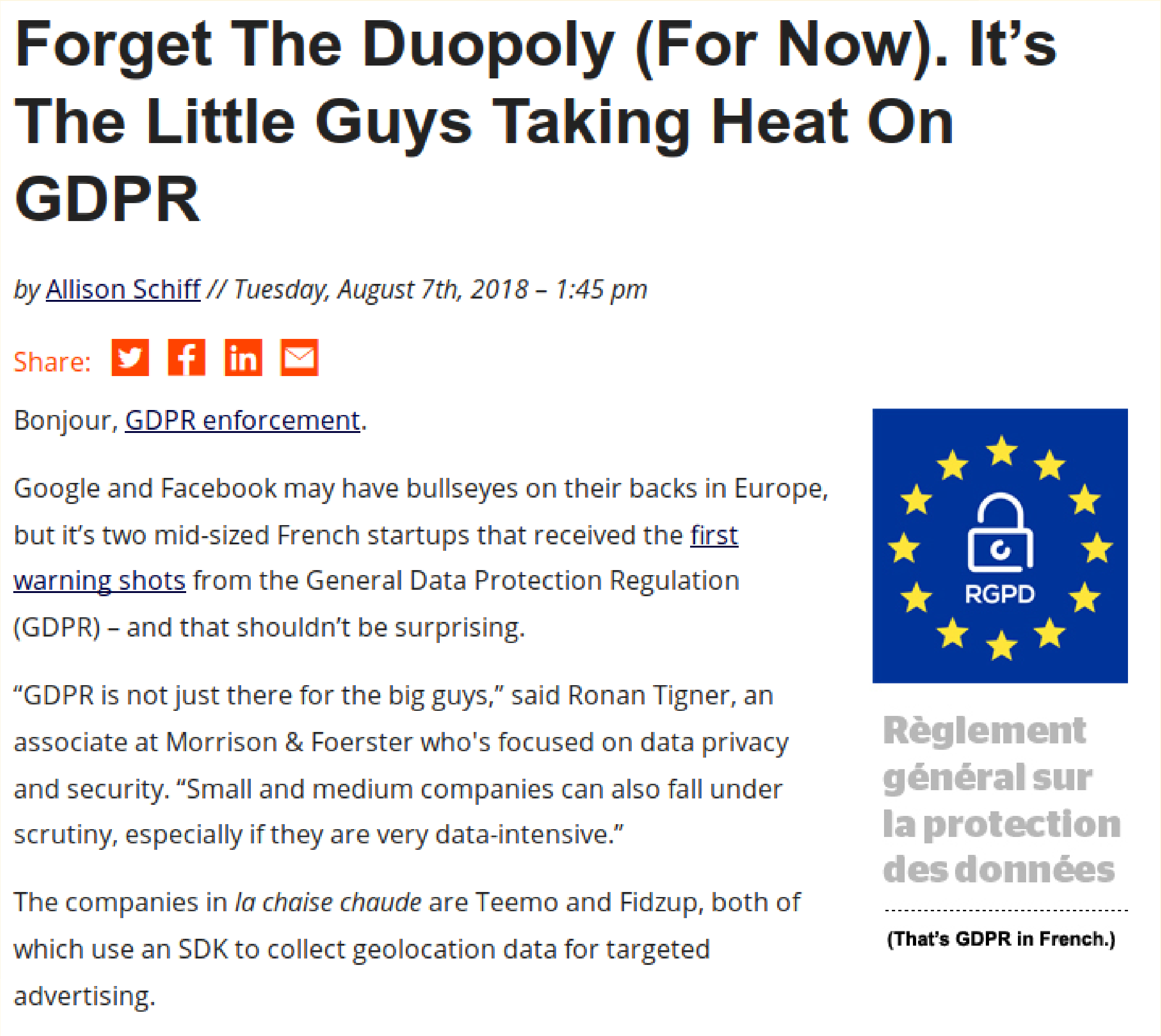
Check out the following example of sonic tracking, via a demo video offered by a tracking company.

Sonic Proximity Targeting

Bienvenue
SOLDES
Bénéficiez de multiples réductions dans notre magasin pendant les soldes
CONTINUER
Bienvenue
SOLDES

- Demo w/ smartphone: https://frama.link/fidvid01
- Video w/ signals: https://frama.link/fidvid-tmt

GDPR Warnings for Fidzup, Teemo



Forget The Duopoly (For Now). It's The Little Guys Taking Heat On GDPR

by Allison Schiff // Tuesday, August 7th, 2018 – 1:45 pm

Share:

Bonjour, GDPR enforcement.

Google and Facebook may have bullseyes on their backs in Europe, but it's two mid-sized French startups that received the first warning shots from the General Data Protection Regulation (GDPR) – and that shouldn't be surprising.

"GDPR is not just there for the big guys," said Ronan Tigner, an associate at Morrison & Foerster who's focused on data privacy and security. "Small and medium companies can also fall under scrutiny, especially if they are very data-intensive."

The companies in *la chaise chaude* are Teemo and Fidzup, both of which use an SDK to collect geolocation data for targeted advertising.

RGPD

Règlement général sur la protection des données

(That's GDPR in French.)

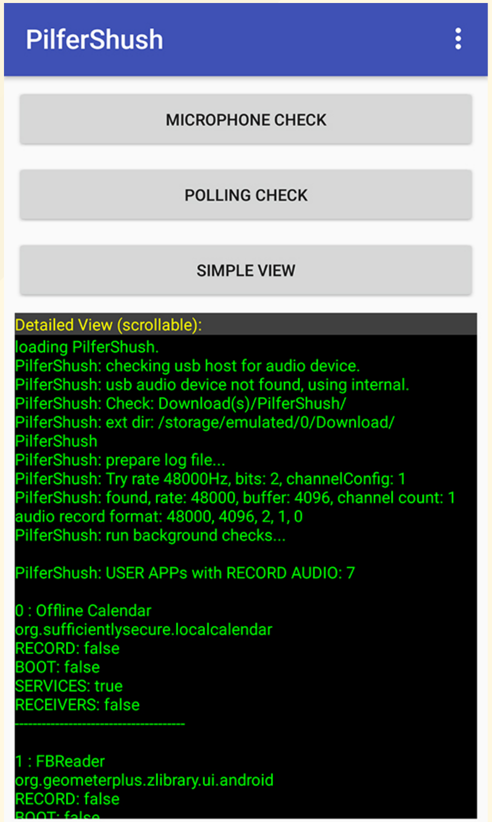
With the help of our PilferShush app, developed by Cityfreqs, we can successfully block these ultrasonic signals.

PilferShush

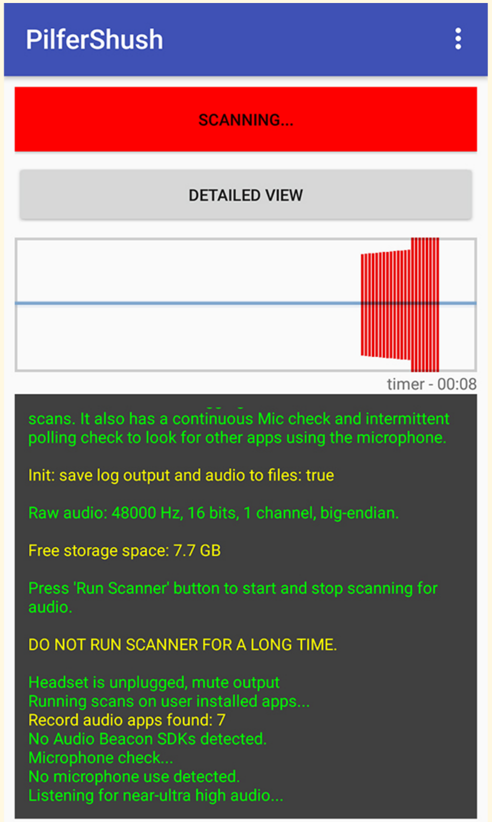
Detects & Blocks Sonic Tracking Signals

https://github.com/YalePrivacyLab/PilferShush_prod

- Android app by Cityfreqs.
- Two versions. PilferShush Jammer is the friendlier one for blocking signals.



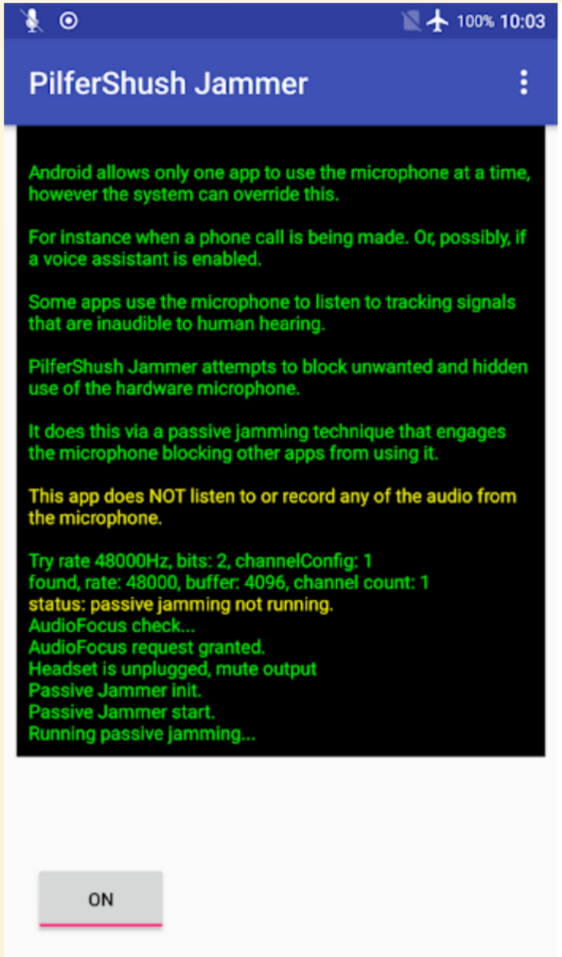
```
Detailed View (scrollable):
loading PilferShush.
PilferShush: checking usb host for audio device.
PilferShush: usb audio device not found, using internal.
PilferShush: Check: Download(s)/PilferShush/
PilferShush: ext dir: /storage/emulated/0/Download/
PilferShush
PilferShush: prepare log file...
PilferShush: Try rate 48000Hz, bits: 2, channelConfig: 1
PilferShush: found, rate: 48000, buffer: 4096, channel count: 1
audio record format: 48000, 4096, 2, 1, 0
PilferShush: run background checks...

PilferShush: USER APPs with RECORD AUDIO: 7

0 : Offline Calendar
org.sufficientlysecure.localcalendar
RECORD: false
BOOT: false
SERVICES: true
RECEIVERS: false
----------------------------------------


1 : FBReader
org.geometerplus.zlibrary.ui.android
RECORD: false
BOOT: false
```



```
scans. It also has a continuous Mic check and intermittent
polling check to look for other apps using the microphone.

Init: save log output and audio to files: true

Raw audio: 48000 Hz, 16 bits, 1 channel, big-endian.

Free storage space: 7.7 GB

Press 'Run Scanner' button to start and stop scanning for
audio.

DO NOT RUN SCANNER FOR A LONG TIME.

Headset is unplugged, mute output
Running scans on user installed apps...
Record audio apps found: 7
No Audio Beacon SDKs detected.
Microphone check...
No microphone use detected.
Listening for near-ultra high audio...
```

Grab the PilferShush Jammer

- Available in F-Droid & Google Play



Android allows only one app to use the microphone at a time, however the system can override this.

For instance when a phone call is being made. Or, possibly, if a voice assistant is enabled.

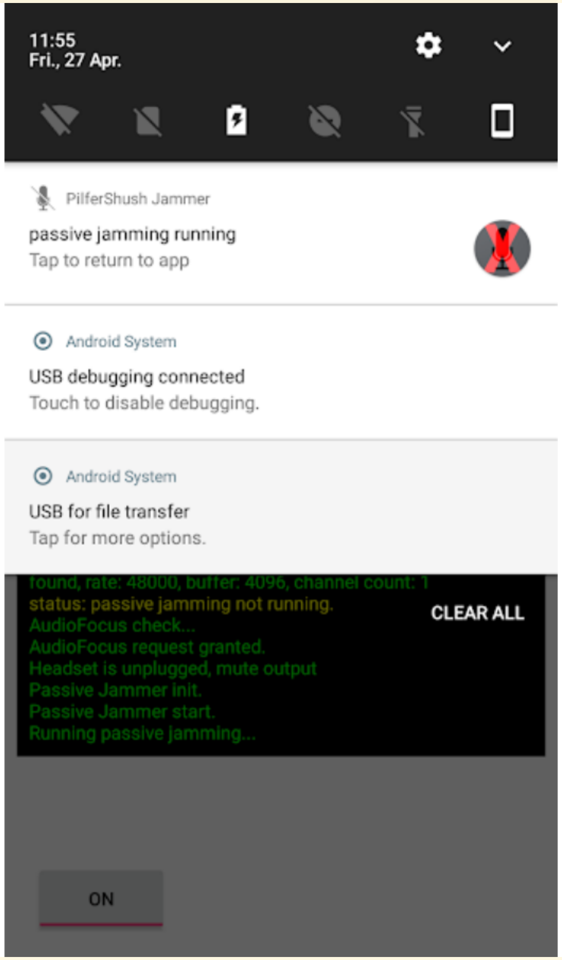
Some apps use the microphone to listen to tracking signals that are inaudible to human hearing.

PilferShush Jammer attempts to block unwanted and hidden use of the hardware microphone.

It does this via a passive jamming technique that engages the microphone blocking other apps from using it.

This app does NOT listen to or record any of the audio from the microphone.

```
Try rate 48000Hz, bits: 2, channelConfig: 1
found, rate: 48000, buffer: 4096, channel count: 1
status: passive jamming not running.
AudioFocus check...
AudioFocus request granted.
Headset is unplugged, mute output
Passive Jammer init.
Passive Jammer start.
Running passive jamming...
```

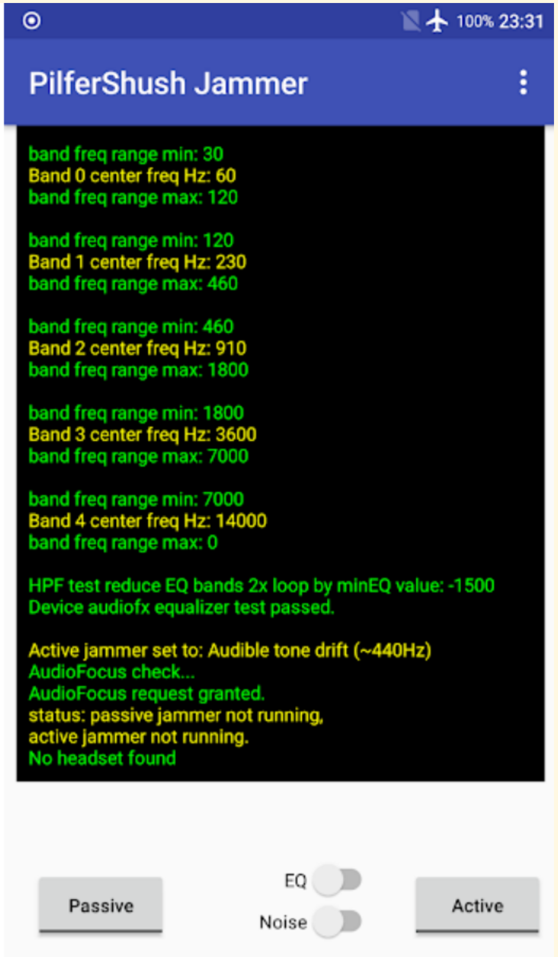


PilferShush Jammer
passive jamming running
Tap to return to app

Android System
USB debugging connected
Touch to disable debugging.

Android System
USB for file transfer
Tap for more options.

```
found, rate: 48000, buffer: 4096, channel count: 1
status: passive jamming not running.
AudioFocus check...
AudioFocus request granted.
Headset is unplugged, mute output
Passive Jammer init.
Passive Jammer start.
Running passive jamming...
```



```
band freq range min: 30
Band 0 center freq Hz: 60
band freq range max: 120

band freq range min: 120
Band 1 center freq Hz: 230
band freq range max: 460

band freq range min: 460
Band 2 center freq Hz: 910
band freq range max: 1800

band freq range min: 1800
Band 3 center freq Hz: 3600
band freq range max: 7000

band freq range min: 7000
Band 4 center freq Hz: 14000
band freq range max: 0

HPF test reduce EQ bands 2x loop by minEQ value: -1500
Device audiofx equalizer test passed.

Active jammer set to: Audible tone drift (~440Hz)
AudioFocus check...
AudioFocus request granted.
status: passive jammer not running,
active jammer not running.
No headset found
```

Beacons are a pervasive adversary to privacy in our physical world.

We can hunt for beacons that may be sending sonic and bluetooth signals.

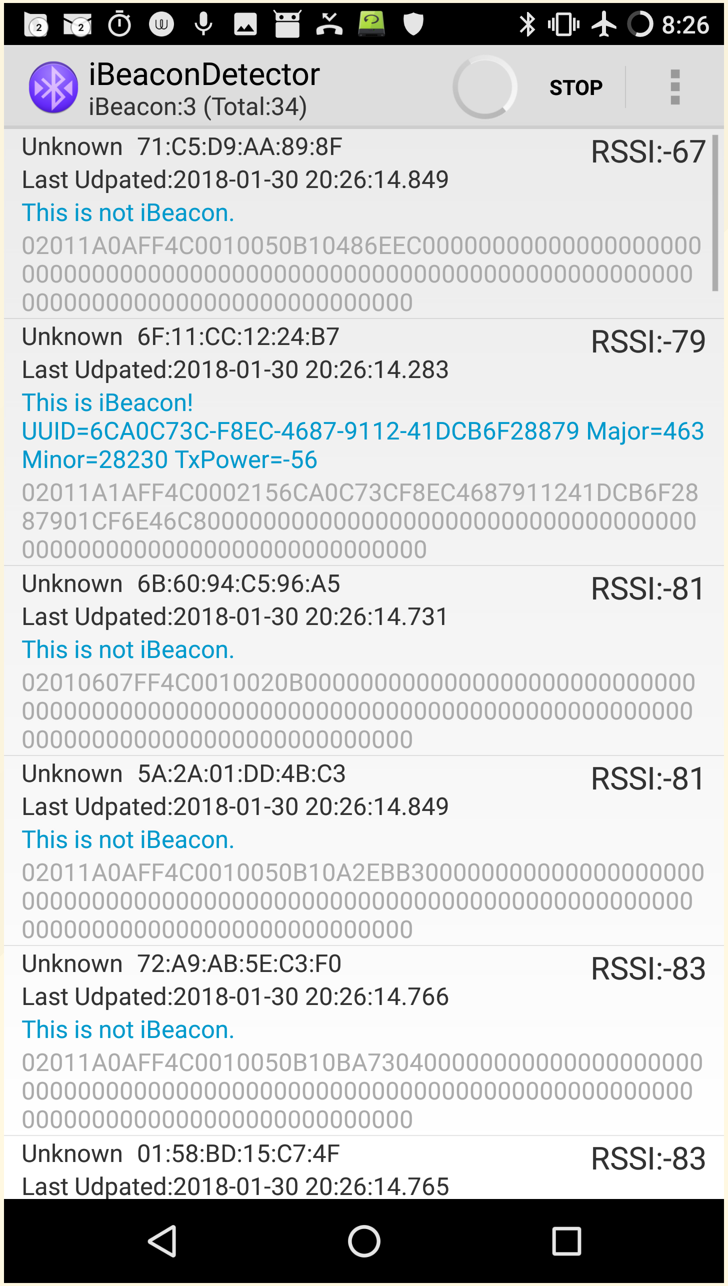
Beacon Hunting

On Android - Beacon Locator, iBeacon Detector

On iOS - Locate Beacon, DIY method

- Sonic tracking is useful in some cases, but bluetooth is more dynamic and widespread.

iBeacon Detected!



iBeaconDetector
iBeacon:3 (Total:34)

Unknown 71:C5:D9:AA:89:8F RSSI:-67
Last Udpated:2018-01-30 20:26:14.849
This is not iBeacon.

```
02011A0AFF4C0010050B10486EEC00000000000000000000
000000000000000000000000000000000000000000000000
0000000000000000000000000000
```

Unknown 6F:11:CC:12:24:B7 RSSI:-79
Last Udpated:2018-01-30 20:26:14.283
This is iBeacon!
UUID=6CA0C73C-F8EC-4687-9112-41DCB6F28879 Major=463
Minor=28230 TxPower=-56

```
02011A1AFF4C0002156CA0C73CF8EC4687911241DCB6F28
87901CF6E46C800000000000000000000000000000000000
00000000000000000000000000000
```

Unknown 6B:60:94:C5:96:A5 RSSI:-81
Last Udpated:2018-01-30 20:26:14.731
This is not iBeacon.

```
02010607FF4C0010020B0000000000000000000000000000
000000000000000000000000000000000000000000000000
0000000000000000000000000000
```

Unknown 5A:2A:01:DD:4B:C3 RSSI:-81
Last Udpated:2018-01-30 20:26:14.849
This is not iBeacon.

```
02011A0AFF4C0010050B10A2EBB300000000000000000000
000000000000000000000000000000000000000000000000
0000000000000000000000000000
```

Unknown 72:A9:AB:5E:C3:F0 RSSI:-83
Last Udpated:2018-01-30 20:26:14.766
This is not iBeacon.

```
02011A0AFF4C0010050B10BA730400000000000000000000
000000000000000000000000000000000000000000000000
0000000000000000000000000000
```

Unknown 01:58:BD:15:C7:4F RSSI:-83
Last Udpated:2018-01-30 20:26:14.765

Remember, you should turn off bluetooth on your devices by default, and be careful about both microphone and bluetooth settings, as well as app permissions.

Thank You!

- Mozilla Open Leaders and Josefina Caro Magaña
- Scott Shapiro, Laurin Weissinger, Jon Oronzo
- Rebecca Crootof, Jack Balkin, Mike Kwet, Yale ISP
- PiRanhaLysis and Exodus Privacy team
- City Frequencies
- Hans-Christoph Steiner and F-Droid team
- Eben Moglen and Danny Haidar, Freedombox Fndn
- Nathan Freitas, Guardian Project