

**CoronApp, Medellín me Cuida y CaliValle Corona
al laboratorio
¿Cómo se hackea CoronApp sin siquiera intentarlo?**

Andres Velásquez
Stéphane Labarthe
FLISOL Bogotá 2020



k-lab@klab-Inspiron-7559: ~



Archivo Editar Ver Buscar Terminal Ayuda

```
k-lab@klab-Inspiron-7559:~$ whoami
```

```
k-lab
```

```
k-lab@klab-Inspiron-7559:~$ whois k-lab
```



“Nada es tan permanente como un programa temporal del gobierno”.

Milton Friedman, economista



K+LAB y los análisis de sitios / apps



Análisis confirma relación de Nation Builder, empresa que ayudó a Trump a llegar a la presidencia, con dos campañas presidenciales en Colombia.



Metodología de análisis (sitios webs y apps)

Características:

- ✓ Análisis de la información y técnico
- ✓ Reproducibles: ¡Hagan lo ustedes también!
- ✓ Se usan softwares libres
- ✓ No intrusivo y legal + información previa
- ✓ Mirando: transparencia/información, seguridad digital ,
privacidad

¡Abramos la caja negra!

¿Porque usar Softwares libres en este contexto?

- Transparencia y confianza: código abierto
- Reproductibilidad: programas accesibles a todos sin costo
- Calidad y eficiencia de las herramientas usadas





¿Que usamos?



Exodus Privacy: Licencia pública GNU, versión 3.0

ClassyShark3xodus: Licencia Apache 2.0

Wireshark: Licencia pública GNU, versión 2.0

OWASP ZAP: Licencia Apache 2.0

Burp Community Edition

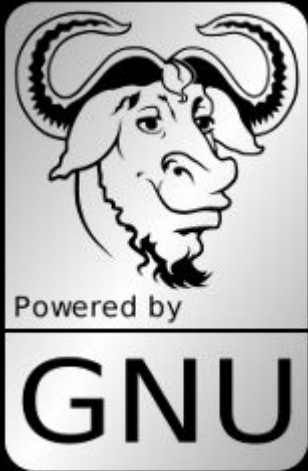
Apktool (Herramienta de ingeniería inversa para APKs)

diff (Para ver las diferencias entre las versiones después de ser des compiladas)

ADB (Android Debug)

para sitios : **Waterfox + LiveHTTP Headers +**

CookieManager+



Análisis estático (sitio web y app)

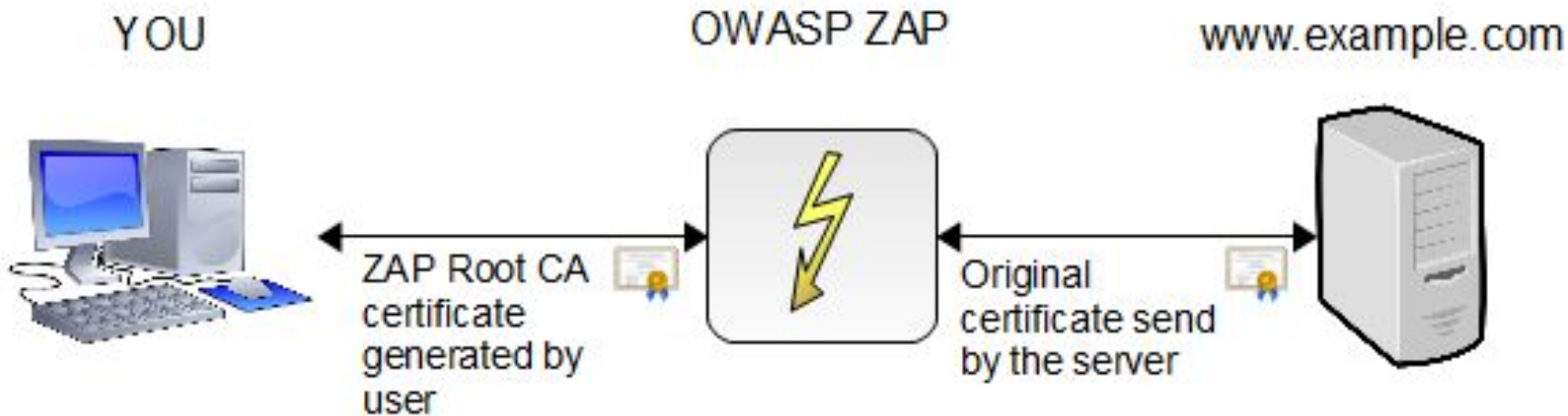
Sitios webs

- dominio y dirección IP (whois)
- certificado
- código fuente (HTML / Javascript)
- cookies

Apps

- información del store
- permisos
- rastreadores
- manifiesto Android
- parte accesible del código fuente

Análisis de flujo/paquetes



Capturing outbound/inbound packets:
Smartphone Apps : HTTPS, DNS
Website : also HTTPS (with LiveHTTP Headers)

Permisos en las Apps (CaliValleCorona)

- App permissions: 35

-
- com.huawei.permission.external_app_settings.USE_COMPONENT
- me.everything.badger.permission.BADGE_COUNT_WRITE
- android.permission.READ_APP_BADGE
- com.oppo.launcher.permission.READ_SETTINGS
- com.htc.launcher.permission.UPDATE_SHORTCUT
- android.permission.READ_PHONE_STATE
- oppo.permission.OPPO_COMPONENT_SAFE
- com.sonyericsson.home.permission.BROADCAST_BADGE
- android.permission.ACCESS_FINE_LOCATION
- android.permission.GET_TASKS
- android.permission.ACCESS_NETWORK_STATE
- ~~com.majeur.launcher.permission.UPDATE_BADGE~~
- me.everything.badger.permission.BADGE_COUNT_READ

- com.sonymobile.home.permission.PROVIDER_INSERT_BADGE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.FOREGROUND_SERVICE
- android.permission.CALL_PHONE
- android.permission.READ_EXTERNAL_STORAGE
- com.htc.launcher.permission.READ_SETTINGS
- com.huawei.android.launcher.permission.CHANGE_BADGE
- android.permission.ACCESS_COARSE_LOCATION
- com.sec.android.provider.badge.permission.READ
- com.huawei.android.launcher.permission.READ_SETTINGS
- com.google.android.gms.permission.ACTIVITY_RECOGNITION
- android.permission.INTERNET
- android.permission.ACCESS_LOCATION_EXTRA_COMMANDS
- com.anddoes.launcher.permission.UPDATE_COUNT
- com.sec.android.provider.badge.permission.WRITE
- android.permission.RECEIVE_BOOT_COMPLETED
- com.huawei.android.launcher.permission.WRITE_SETTINGS
- android.permission.ACCESS_BACKGROUND_LOCATION
- android.permission.ACTIVITY_RECOGNITION
- android.permission.WAKE_LOCK
- com.oppo.launcher.permission.WRITE_SETTINGS
- android.permission.BLUETOOTH

Permisos/tackers CoronApp (Exodus)

Exodus Privacy

CoronApp

2 Trackers

16 Permissions

Installed Version: 1.2.37

Created By

This report has been created the 23 de abril de 2020

See on Exodus Privacy

See on Google Play

2 Trackers

We have found code signature of the following trackers in the application:

- Google CrashLytics >
- Google Firebase Analytics >

A tracker is a piece of software meant to collect data about you or your usages. [Learn more...](#)

16 Permissions

We have found the following permissions in the application:

- MAPS_RECEIVE
- INTERNET ▶
- ACCESS_NETWORK_STATE ▶
- ACCESS_COARSE_LOCATION ▶

- RECEIVE_BOOT_COMPLETED
ejecutarse al inicio
- FOREGROUND_SERVICE
- CALL_PHONE ▶
llamar directamente a números de teléfono
- BLUETOOTH ▶
vincular con dispositivos Bluetooth
- ACCESS_WIFI_STATE
ver conexiones Wi-Fi
- CHANGE_WIFI_STATE
conectarse a redes Wi-Fi y desconectarse
- BLUETOOTH_PRIVILEGED ▶
android.permission.BLUETOOTH_PRIVILEGED

- BLUETOOTH_ADMIN ▶
acceder a los ajustes de Bluetooth
- WAKE_LOCK ▶
impedir que el teléfono entre en modo de suspensión
- RECEIVE ▶
recibir datos de Internet
- BIND_GET_INSTALL_REFERRER_SERVICE ▶
API Install Referrer de Play

The icon ! indicates a 'Dangerous' or 'Special' level according to [Google's protection levels](#).

Permissions are actions the application can do on your phone. [Learn more...](#)



Análisis de tráfico en Coronapp - encontrando una vulnerabilidad 1.

request

The screenshot displays a list of network requests. The 210th request is highlighted in orange and is a POST request to `/household/create` with a status of 200 and content type of JSON. Below the list, the 'Request' tab is selected, showing the raw HTTP request details:

```
1 POST /household/create HTTP/1.1
2 app_token: d41d8cd98f00b204e9800998ecf8427e
3 Content-Type: application/json
4 Content-Length: 969
5 Host: 52.87.234.39:5000
6 Connection: close
7 Accept-Encoding: gzip, deflate
8 User-Agent: okhttp/4.2.2
9
10 {"firstname":"usuario2 prueba","lastname":"test","phone":"","client":"api","dob":"1900-01-01","gender":"Hombre","app_token":"d41d8cd98f00b204e9800998ecf8427e","race":"Rom-Gitano","document_type":"CC","document_number":"12345678","country":"Colombia","city":"Bogota","state":"Bogota D.C.","platform":"android","relationship":"Bisnieto","user":"5e83a9e0ebc6f0001072d65"}
```

response

The screenshot displays the same list of network requests as above. The 210th request is highlighted in orange. Below the list, the 'Response' tab is selected, showing the raw HTTP response details:

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.17.9
3 Date: Tue, 31 Mar 2020 20:47:35 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: close
6 Content-Length: 569
7
8 {"error":false,"message":"Household member Created","member":{"id":"5e83ac67ebc6f0001072d80","picture":0,"dob":"1900-01-01T00:00:00","city":"Bogota","state":"Bogota D.C.","gender":"Hombre","firstname":"usuario2 prueba","user":"5e83a9e0ebc6f0001072d65","platform":"android","client":"api","country":"Colombia","race":"Rom-Gitano","relationship":"Bisnieto","lastname":"test","app_token":"d41d8cd98f00b204e9800998ecf8427e","createdAt":"2020-03-31T20:47:35.9820258+00:00","updatedAt":"2020-03-31T20:47:35.9820296+00:00","document_number":"12345678","document_type":"CC"}}
```

Análisis de tráfico en Coronapp - encontrando una vulnerabilidad. 2.

request

No.	Method	URL	Status	Size	Content-Type	Other
210	POST	/household/create	✓	200	734	JSON
211	GET	/user/household/5e83a9e0ebc6fc0001072d65	✓	200	2527	JSON
214	GET	/generate_204		204	102	
215	GET	/generate_204		204	309	
216	POST	/auth/devicekey	✓	400	2156	HTML Error 400 (Not Found)!!!

```
1 GET /user/household/5e83a9e0ebc6fc0001072d65 HTTP/1.1
2 Host: 52.87.234.39:5000
3 User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; Android SDK built for x86_64 Build/PSR1.180720.093)
4 Accept-Encoding: gzip, deflate
5 Connection: close
6 Accept: */*
7 app_token: d41d8cd98f00b204e9800998ecf8427e
8 user_token:
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmRkxwVWVmbmFtZSI6IjVlODNhOWwzZWJmNmZjMDAwMTA3MmQzIiwiaWF0IjoiMjAyMC03LTM1TjAzOjM3LjE5ODUyMjAwMDh9.UPE_NdBRtNqYzA
  yLxhIPmN8RkoFAB3pmx-tFbwAMTJC
9 Content-Type: application/json
10
```

response

No.	Method	URL	Status	Size	Content-Type	Other
211	GET	/user/household/5e83a9e0ebc6fc0001072d65	✓	200	2527	JSON
214	GET	/generate_204		204	102	
215	GET	/generate_204		204	309	
216	POST	/auth/devicekey	✓	400	2156	HTML Error 400 (Not Found)!!!

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.17.9
3 Date: Tue, 31 Mar 2020 20:47:39 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: close
6 Content-Length: 2361
7
8 [{"error": "false", "data": [{"surveys": [{"id": "5e83a9f9ebc6fc0001072d67", "platform": "android", "no_symptom": "Y", "lon": -122.084, "lat": 37.4219983, "app_token": "d41d8cd98f00b204e9800998ecf8427e", "user": "5e83a9e0ebc6fc0001072d65", "week_of": "2020-03-31T20:37:13.866Z", "coordinates": [{"lon": -122.084, "lat": 37.4219983}], "createdAt": "2020-03-31T20:37:13.866Z", "updatedAt": "2020-03-31T20:37:13.866Z", "client": "api", "hadTravelledAbroad": false, "startDate": "0001-01-01T00:00:00Z", "hadContagiousContact": false, "hadHealthCare": false}, {"id": "5e83a9f9ebc6fc0001072d66", "platform": "android", "no_symptom": "Y", "lon": -122.084, "lat": 37.4219983, "app_token": "d41d8cd98f00b204e9800998ecf8427e", "user": "5e83a9e0ebc6fc0001072d65", "week_of": "2020-03-31T20:37:13.866Z", "coordinates": [{"lon": -122.084, "lat": 37.4219983}], "createdAt": "2020-03-31T20:37:13.866Z", "updatedAt": "2020-03-31T20:37:13.866Z", "client": "api", "hadTravelledAbroad": false, "startDate": "0001-01-01T00:00:00Z", "hadContagiousContact": false, "hadHealthCare": false}], "user": {"id": "5e83a9e0ebc6fc0001072d65", "picture": "0", "dob": "1900-01-01T00:00:00Z", "city": "Bogota", "email": "test2@karisma.org.co", "state": "Bogota D.C.", "gender": "Masculino", "firstName": "usuario prueba", "platform": "android", "country": "Colombia", "race": "Escoge una opción", "gcm_token": "cva0bujw-3E-4P401bnpX0tupNtucdCnyc_281E74555f0w7fBU2fy_3BA0VjH2osPOYmWzfdNSP-fs0AGc55gH-1i69uW4HywbASXqsB8kqgH4u10egT0EChIH41FY0yDyKPBcRpUy9cwkT", "lastName": "test", "week_of": "2020-04-01T20:36:48.512Z", "active": "Y", "isAdmin": false, "app": "d41d8cd98f00b204e9800998", "age": 120, "ageGroup": "80", "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmRkxwVWVmbmFtZSI6IjVlODNhOWwzZWJmNmZjMDAwMTA3MmQzIiwiaWF0IjoiMjAyMC03LTM1TjAzOjM3LjE5ODUyMjAwMDh9.UPE_NdBRtNqYzA yLxhIPmN8RkoFAB3pmx-tFbwAMTJC", "device_id": "4dc184eb13a57495", "document_number": "12345678", "document_type": "CC", "createdAt": "2020-03-31T20:36:48.512Z", "updatedAt": "2020-03-31T20:36:48.512Z", "id": "5e83a9f9ebc6fc0001072d60", "picture": "0", "dob": "1900-01-01T00:00:00Z", "city": "Bogota", "state": "Bogota D.C.", "gender": "Hombre", "firstName": "usuario2 prueba", "platform": "android", "country": "Colombia", "race": "Rom-Gitano", "relationship": "Bisnieto", "lastName": "test", "appToken": "d41d8cd98f00b204e9800998ecf8427e", "createdAt": "2020-03-31T20:47:35.982Z", "updatedAt": "2020-03-31T20:47:35.982Z", "documentNumber": "12345678", "documentType": "CC"}}]}
9
```

Vulnerabilidad Medellin <-> EPM



```
GET https://epm.adminfo.net/vsmart/services/epm/index.php/dataDir/?id=44951&_ =1586810468367 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Origin: https://medellin.gov.co
Connection: keep-alive
Referer: https://medellin.gov.co/medellinmecuida
Host: epm.adminfo.net
```

```
HTTP/1.1 200 OK
Date: Mon, 13 Apr 2020 20:42:33 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1;mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=631138519
X-Permitted-Cross-Domain-Policies: none
Content-Length: 413
Connection: close
Content-Type: application/json; charset=UTF-8
```

```
{"identificacion": "4-███", "nombre_cliente": "CARDONA, JORGE ENRIQUE ██████████", "cod_ciudad": "1700501001", "desc_ciudad": "MEDELLIN",
"cod_dpto": "17005", "desc_dpto": "ANTIOQUIA", "coordenada_x": "-75.601952", "coordenada_y": "6.█████4", "direccion":
"CR ██████████ 1)", "cod_categoria": "1", "desc_categoria": "RESIDENCIAL", "cod_estrato": "4", "desc_estrato": "ESTRATO 4",
"riesgo": "1 Bajo", "val_factura": "190253.10"}
```



Vigilancia intensa de CaliValleCorona



File Edit View Analyse Report Tools Import Online Help

Safe Mode

Quick Start Request Response Sites History Search Alerts HTTP Sessions Output

Filter: OFF Export

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size R...	Highest...	Note	Tags
371	4/13/20, 10:57:43 PM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	408 ms	172 by...	Infor...		JSON
382	4/13/20, 11:28:20 PM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	399 ms	172 by...	Infor...		JSON
390	4/13/20, 11:43:20 PM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	515 ms	172 by...	Infor...		JSON
397	4/14/20, 12:13:59 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	379 ms	172 by...	Infor...		JSON
409	4/14/20, 12:29:00 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	403 ms	172 by...	Infor...		JSON
430	4/14/20, 12:59:37 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	468 ms	172 by...	Infor...		JSON
436	4/14/20, 1:14:37 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	502 ms	172 by...	Infor...		JSON
448	4/14/20, 1:45:15 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	438 ms	172 by...	Infor...		JSON
454	4/14/20, 2:00:16 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	510 ms	172 by...	Infor...		JSON
463	4/14/20, 2:30:52 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	436 ms	172 by...	Infor...		JSON
478	4/14/20, 2:45:53 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	504	Gatew...	20.12 s	207 by...			
480	4/14/20, 2:46:59 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	291 ms	172 by...	Infor...		JSON
490	4/14/20, 3:16:29 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	551 ms	172 by...	Infor...		JSON
497	4/14/20, 3:31:30 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	405 ms	172 by...	Infor...		JSON
513	4/14/20, 4:02:14 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	411 ms	172 by...	Infor...		JSON
519	4/14/20, 4:17:15 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	476 ms	172 by...	Infor...		JSON
529	4/14/20, 4:47:57 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	406 ms	172 by...	Infor...		JSON
533	4/14/20, 5:02:57 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	404 ms	172 by...	Infor...		JSON
547	4/14/20, 5:33:40 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	477 ms	172 by...	Infor...		JSON
555	4/14/20, 5:48:41 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	418 ms	172 by...	Infor...		JSON
574	4/14/20, 6:19:22 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	380 ms	172 by...	Infor...		JSON
585	4/14/20, 6:34:22 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	504	Gatew...	20.21 s	207 by...			
586	4/14/20, 6:35:29 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	282 ms	172 by...	Infor...		JSON
597	4/14/20, 7:04:59 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	404 ms	172 by...	Infor...		JSON
601	4/14/20, 7:20:00 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	391 ms	172 by...	Infor...		JSON
618	4/14/20, 7:50:37 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	496 ms	172 by...	Infor...		JSON
624	4/14/20, 8:05:37 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	415 ms	172 by...	Infor...		JSON
634	4/14/20, 8:36:21 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	378 ms	172 by...	Infor...		JSON
645	4/14/20, 8:51:22 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	481 ms	172 by...	Infor...		JSON
657	4/14/20, 9:22:01 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	423 ms	172 by...	Infor...		JSON
660	4/14/20, 9:37:02 AM	POST	https://api.calvallecorona.com/api/user-ggpps/reporte	201	Created	397 ms	172 by...	Infor...		JSON

Alerts 1 0 0 0 2 Primary Proxy: 192.168.0.17:8080

Current Scans 0 0 0 0 0 0 0 0 0 0 0 0

Usando apktool



```
android:screenOrientation="portrait" android:theme="@style/Theme.NoActionBar" />
<meta-data android:name="com.google.android.geo.API_KEY" android:value="AIzaSyBap804eY3xDn_y_InjrybKkDsp3c6bDEw"/>
<uses-library android:name="org.apache.http.legacy" android:required="false"/>
<service android:enabled="true" android:exported="false" android:label="@string/app_name"
android:name="com.hypelabs.hype.HypeService"/>
<provider android:authorities="co.gov.ins.guardianes.crashlyticsinitprovider" android:exported="false"
android:initOrder="90" android:name="com.crashlytics.android.CrashlyticsInitProvider"/>
<service android:directBootAware="true" android:exported="false"
android:name="androidx.room.MultiInstanceInvalidationService"/>
<service android:directBootAware="true" android:exported="false"
android:name="com.google.firebase.components.ComponentDiscoveryService">
<meta-data
android:name="com.google.firebase.components:com.google.firebase.analytics.connector.internal.AnalyticsConnectorRegistrar"
android:value="com.google.firebase.components.ComponentRegistrar"/>
<meta-data android:name="com.google.firebase.components:com.google.firebase.iid.Registrar"
android:value="com.google.firebase.components.ComponentRegistrar"/>
</service>
<receiver android:exported="true" android:name="com.google.firebase.iid.FirebaseInstanceIdReceiver"
android:permission="com.google.android.c2dm.permission.SEND">
<intent-filter>
<action android:name="com.google.android.c2dm.intent.RECEIVE"/>
</intent-filter>
</receiver>
<activity android:exported="false" android:name="com.google.android.gms.common.api.GoogleApiActivity" />
```

AP

Top Stories Topics

PRESS RELEASE: Paid content

HypeLabs' Contact-Tracing Technology Focused on Privacy Now Available for Immediate Deployment at No Cost for All Countries

April 14, 2020

CovidApp has already been tested and deployed in some countries in Latin America such as [Colombia](#), the first nation to adopt the system showing the lowest numbers of infected patients in the region and is managing the flattening of the curve.



Fundación
Karisma

¡Gracias!



This presentation has a
[licencia de Creative Commons Reconocimiento 4.0 Internacional](https://creativecommons.org/licenses/by/4.0/).