

Threat research in Covid context

Analyzing websites and Apps

Andres Velásquez
Stéphane Labarthe
Webinar CIVICERT, June 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
```

“Nothing is so permanent as a temporary government program.”

Milton Friedman

Colombia locals and central governments have developed a lot of websites and apps in response to Covid crisis



We decided to analyze some of them

Methodology (websites and apps)

Characteristics:

- ✓ Analysis of public information (legal) and technical analysis
 - ✓ Reproducible: ¡Do it Yourself!
 - ✓ Free software (mainly)
 - ✓ Non intrusive and legal + previous information + non public report sent to the government before publication
 - ✓ Main points: transparency/information, digital security, privacy.
-

When we found some serious vulnerabilities, we didn't exploit them (could be a crime in Colombia) but worked with Access Now who verified them.

¿Why do we use free software in this context?

- Transparency and trust: Open Source
- Replicable: Access to software without cost, "Do it Yourself" approach
- Quality and efficiency.





¿What do we use? <K+LAB>

SEGURIDAD DIGITAL Y PRIVACIDAD

Exodus Privacy: permissions and trackers

Wireshark: packet capture

OWASP ZAP: HTTP(S) capture (MITM)

Burp Community Edition: app emulation and websecurity

Apktool (Reverse engineering for APKs)

diff (differences between 2 versions of an ap)

ADB (Android Debug)

Websites: **Waterfox + LiveHTTP Headers + CookieManager±**

Iphones: Apple Configurator (Console) + OWASP ZAP



Static analysis (website and app)

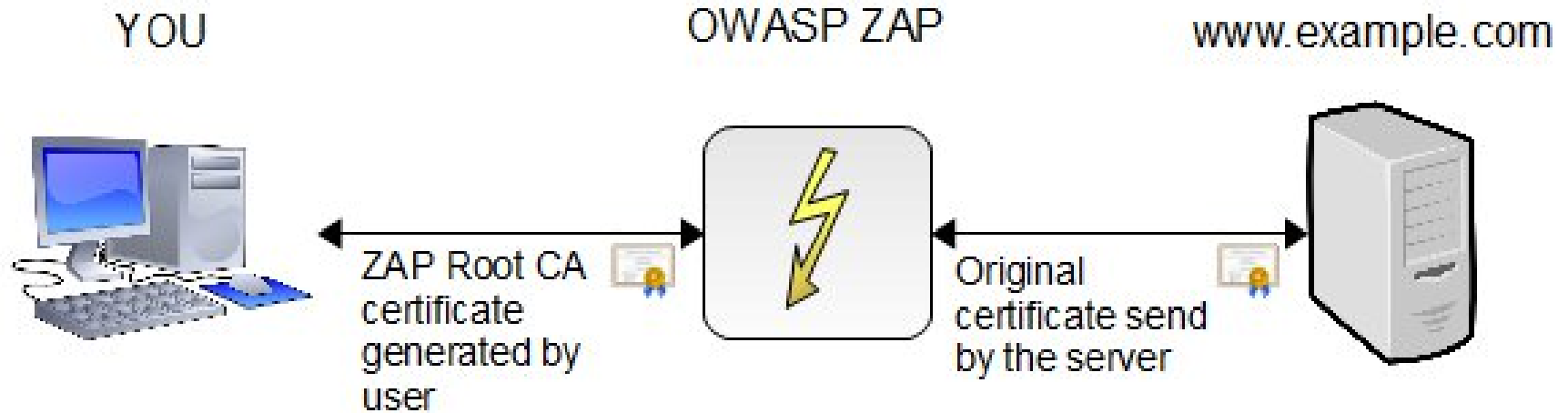
Websites

- Public information (T&C, privacy policy, etc.)
- Domain and IP address (host/nslookup, whois)
- Certificate
- Source code (HTML / Javascript)
- Cookies

Apps

- Store information
- Permissions
- Trackers
- Android manifest
- Disassembled source code

Packet analysis with OWASP ZAP



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

Installing a root Certificate Authority (ZAP, MITMx, etc.)

Emulation (Burp or other)	Android < 7	Android ≥ 7	iPhone
Root CA can be installed as "system root CA" using ADB easily	Root CA can be installed as "user root CA" → maybe the easiest way	Root CA need to be installed as "system root CA" → need to root the phone and use ADB	Create a Business Apple account and register device as "supervised device" Use Apple Configurator to create profile in the phone with the root CA

Permissions in 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

Permissions and 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 ➤
tener acceso completo a la red
- ACCESS_NETWORK_STATE ➤
ver conexiones de red
- ACCESS_COARSE_LOCATION ➤
acceder a tu ubicación aproximada (basada en red)

- 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...](#)



Data sent by Coronapp with HTTP



SEGURIDAD DIGITAL Y PRIVACIDAD

Registro

Nombres

Fundacion Karisma

Apellidos

TestNotomarEnCuenta

Tipo de documento

Cédula de Ciudadanía

Número de documento

1234567890

Celular

3123456789

Wireshark · Packet 535 · Captura WireShark 2 (Registro).pcap

· Frame 535: 925 bytes on wire (7400 bits), 925 bytes captured (7400 bits) on interface 0
· Ethernet II, Src: MurataMa_18:e0:1f (b8:d7:af:18:e0:1f), Dst: klab-Inspiron-7559.local (84:ef:18:ce:6a:21)
· Internet Protocol Version 4, Src: 10.42.0.202 (10.42.0.202), Dst: apicovid.and.gov.co (52.87.234.39)
· Transmission Control Protocol, Src Port: 57220, Dst Port: 5000, Seq: 1, Ack: 1, Len: 859
· IPA protocol ip.access, type: unknown 0x53
DataLen: 20559
Protocol: Unknown (0x53)

```
0000  84 ef 18 ce 6a 21 b8 d7 af 18 e0 1f 08 00 45 00  ...j!... ..E-
0010  03 8f 5f 52 40 00 40 06 ae a4 0a 2a 00 ca 34 57  .._R@.@...*.4W
0020  ea 27 df 84 13 88 c6 a8 74 62 c1 10 4a 54 80 18  ...tbaJT...
0030  02 ad 37 4e 00 00 01 01 08 0a 00 13 2b 3e 06 1e  ...7N....+>...
0040  81 c5 50 4f 53 54 20 2f 75 73 65 72 2f 63 72 65  ...POST / user/cre
0050  61 74 65 20 48 54 54 50 2f 31 2e 31 0d 0a 61 70  ate HTTP /1.1 ap
0060  70 5f 74 6f 6b 65 6e 3a 20 64 34 31 64 38 63 64  p_token: d41d8c
0070  39 38 66 30 30 62 32 30 34 65 39 38 30 30 39 39  98f00b20 4e980099
0080  38 65 63 66 38 34 32 37 65 0d 0a 43 6f 6e 74 65  8ecf8427 e Conte
0090  6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61  nt-Type: applica
00a0  74 69 6f 6e 2f 6a 73 6f 6e 0d 0a 43 6f 6e 74 65  tion/json Conte
00b0  6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 36 0d 0a  nt-Lengt h: 626
00c0  48 6f 73 74 3a 20 61 70 69 63 6f 76 69 64 2e 61  Host: ap icovid.a
00d0  6e 64 2e 67 6f 76 2e 63 6f 3a 35 30 30 30 0d 0a  nd.gov.c o:5000
00e0  43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70  Connecti on: Keep
00f0  2d 41 6c 69 76 65 0d 0a 41 63 63 65 70 74 2d 45  -Alive.. Accept-E
0100  6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 0d 0a 55  ncoding: gzip..U
0110  73 65 72 2d 41 67 65 6e 74 3a 20 6f 6b 68 74 74  ser-Agen t: okhtt
0120  70 2f 34 2e 32 2e 32 0d 0a 0d 0a 7b 22 66 69 72  p/4.2.2. ...{"fir
0130  73 74 6e 61 6d 65 22 3a 22 46 75 6e 64 61 63 69  stname": "Fundaci
0140  6f 6e 20 4b 61 72 69 73 6d 61 22 2c 22 6c 61 73  on Karis ma","las
0150  74 6e 61 6d 65 22 3a 22 54 65 73 74 4e 6f 74 6f  tname": "TestNot
0160  6d 61 72 45 6e 43 75 65 6e 74 61 22 2c 22 64 6f  marEncCue nta","do
0170  63 75 6d 65 6e 74 5f 74 79 70 65 22 3a 22 43 43  ument_t ype":"CC
0180  22 2c 22 64 6f 63 75 6d 65 6e 74 5f 6e 75 6d 62  ","docum ent_numb
0190  65 72 22 3a 22 31 32 33 34 35 36 37 38 39 30 22  er":"123 4567890"
01a0  2c 22 70 68 6f 6e 65 22 3a 22 33 31 32 33 34 35  ,"phone" : "312345
01b0  36 37 38 39 22 2c 22 65 6d 61 69 6c 22 3a 22 74  6789","e mail": "t
01c0  65 73 74 40 6b 61 72 69 73 6d 61 2e 6f 72 67 2e  est@kari sma.org.
01d0  63 6f 22 2c 22 70 61 73 73 77 6f 72 64 22 3a 22  co","pas sword":
01e0  41 7a 65 72 74 79 37 38 22 2c 22 63 6c 69 65 6e  Azerty78 ","clien
01f0  74 22 3a 22 61 70 69 22 2c 22 67 65 6e 64 65 72  t": "api", "gender
0200  22 3a 22 46 65 6d 65 6e 69 6e 6f 22 2c 22 61 70  ": "Femen ino", "ap
0210  70 5f 74 6f 6b 65 6e 22 3a 22 64 34 31 64 38 63  p token" : "d41d8c
```

Data sent by GABO (Bogota, mobility report) with HTTPS



Reportar Movilidad

Localidad de residencia:

Chapinero

Hora de Salida:

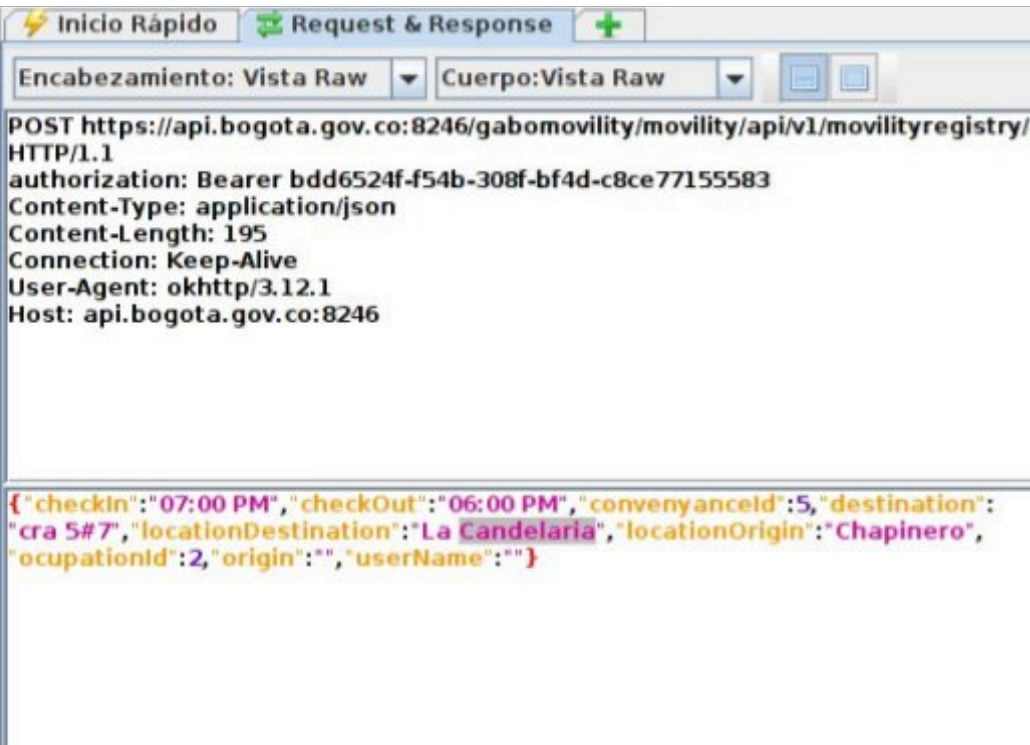
06:00 PM

Localidad de Destino:

La Candelaria

cra 5#7

Hora de Llegada al destino:



Traffic analysis on Coronapp - finding a vulnerability

1.

request

Wireshark packet capture showing an HTTP POST request to /household/create. The packet list on the left shows the request at offset 210. The packet details pane on the right shows the request structure:

```
1 POST /household/create HTTP/1.1
2 app_token: d41d8cd98f00b204e9800998ecf8427e
3 Content-Type: application/json
4 Content-Length: 369
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":"5e83a9e0ebc6fc0001072d65"}
```

response

Wireshark packet capture showing an HTTP 200 OK response. The packet list on the left shows the response at offset 210. The packet details pane on the right shows the response structure:

```
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":"5e83ac67ebc6fc0001072d80","picture":0,"dob":"1900-01-01T00:00:00","city":"Bogota","state":"Bogota D.C.","gender":"Hombre","firstname":"usuario2 prueba","user":"5e83a9e0ebc6fc0001072d65","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"}}
```

Traffic analysis on Coronapp - finding a vulnerability.

2.

request

210	http://52.87.234.39:5000	POST	/household/create	✓	200	734	JSON	
211	http://52.87.234.39:5000	GET	/user/household/5e83a9e0ebc6fc0001072d65		200	2527	JSON	
214	http://connectivitycheck.gstatic.com	GET	/generate_204		204	102		
215	https://www.google.com	GET	/generate_204		204	309		
216	https://android.clients.google.com	POST	/auth/devicekey	✓	400	2156	HTML	Error 400 (Not Found)!!!

Request	Response
Raw	Headers
Hex	

```
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.eyJ1bm9kdmVmbWZlZSI6IjVlODNhOWUwZWJjNmZjMDAwMTA3MmQ2NSIsIn5iOiI1ZiI6MTU4NTY4NzAwOwIjXkhwIjoxNTg4MjY0MTU0ODcwMDh9.UPE_NdBRTNqYzA
  yLxhIPmN8RkoFAB3pmx-tFbwAMTJC
9 Content-Type: application/json
10
```

response

211	http://52.87.234.39:5000	GET	/user/household/5e83a9e0ebc6fc0001072d65		200	2527	JSON	
214	http://connectivitycheck.gstatic.com	GET	/generate_204		204	102		
215	https://www.google.com	GET	/generate_204		204	309		
216	https://android.clients.google.com	POST	/auth/devicekey	✓	400	2156	HTML	Error 400 (Not Found)!!!

Request	Response
Raw	Headers
Hex	

```
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}], "created_at": "2020-03-31T20:37:13.866Z", "updated_at": "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": "2020-03-31T20:37:13.858Z", "coordinates": [{"lon": -122.084, "lat": 37.4219983}], "created_at": "2020-03-31T20:37:13.858Z", "updated_at": "2020-03-31T20:37:13.858Z", "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": "c2u43ujw-3E:APA91bnpX0XuWpvtu0Cnyc-281745S5fwt7BUZfey-3BA0YJh2osPOYmWzFDNSP-fsa0Agz65gH-1i69uW4hyebwBAsXq5B8kqqgH4w10egT0EcIH41FY8yDyKPC8RpUvY9cwkT", "lastName": "test", "week_of": "2020-04-01T20:36:48.512Z", "active": "Y", "isAdmin": false, "app": "d41d8cd98f00b204e9800998ecf8427e", "age": 120, "ageGroup": "80", "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bm9kdmVmbWZlZSI6IjVlODNhOWUwZWJjNmZjMDAwMTA3MmQ2NSIsIn5iOiI1ZiI6MTU4NTY4NzAwOwIjXkhwIjoxNTg4MjY0MTU0ODcwMDh9.UPE_NdBRTNqYzAylXhIPmN8RkoFAB3pmx-tFbwAMTJC", "device_id": "4dc1b4eb13a5f495", "document_number": "12345678", "document_type": "CC", "created_at": "2020-03-31T20:36:48.512Z", "updated_at": "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", "created_at": "2020-03-31T20:47:35.982Z", "updated_at": "2020-03-31T20:47:35.982Z", "documentNumber": "12345678", "documentType": "CC"}]}]
```


Vulnerability in Medellin <-> EPM



```
GET https://epm.adminfo.net/vsmart/services/epm/index.php/dataDir?id=4[REDACTED]&_k=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[REDACTED]", "nombre_cliente": "CARDOL[REDACTED] S", "cod_ciudad": "1700501001", "desc_ciudad": "MEDELLIN",
  "cod_dpto": "17005", "desc_dpto": "ANTIOQUIA", "coordenada_x": "-75.601952", "coordenada_y": "6.[REDACTED]4", "direccion":
  "CR 64 N° 45 E - 82 (INTERSECCION 501)", "cod_categoria": "1", "desc_categoria": "RESIDENCIAL", "cod_estrato": "4", "desc_estrato": "ESTRATO 4",
  "riesgo": "1 Bajo", "val_factura": "190253.10" }
```

Close surveillance in CaliValleCorona

K

File Edit View Analyse Report Tools Import Online Help

Safe Mode

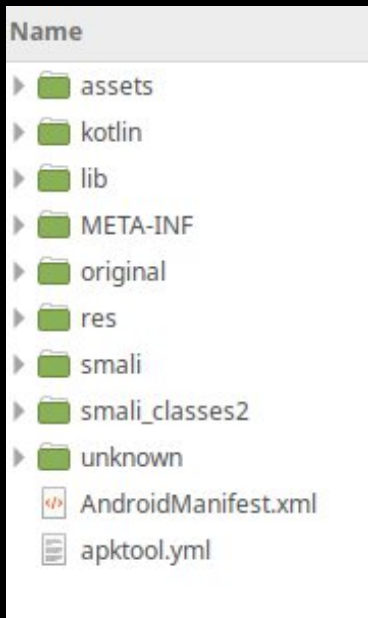
Quick Start Request Response Sites History Search Alerts HTTP Sessions Output

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 0 2 Primary Proxy: 192.168.0.17:8080

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



using 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="99" 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>

```



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.

Tracking cookies in Bogota webforms



	Domain	Name	Content	HTTP Only	Secure	Expires
<input type="checkbox"/>	.truepush.com	tp	j%3A%225ec5f84453a1859fc05a1681%22	Yes	No	20 de marzo de 2030
<input checked="" type="checkbox"/>	.truepush.com	sessionId	92844665-54e8-59ed-a188-067614750022	Yes	No	20 de marzo de 2030
<input type="checkbox"/>	.truepush.com	XSRF-TOKEN	3954f492-40d0-5c19-95b8-c734bbb28148	No	No	20 de marzo de 2030

Domain	Name	Content	Expires
.office.com	MUID	3E9DD3B0675A627023DFDD54664E6328	3 de julio de 2021
.c.bing.com	SRM_B	3E9DD3B0675A627023DFDD54664E6328	3 de julio de 2021
.bing.com	MUID	3E9DD3B0675A627023DFDD54664E6328	3 de julio de 2021
forms.office.com	MSFPC	GUID=2b3c3c7994b844d5afcc9f9a31bec967&HASH=2b3c&LV=20...	8 de junio de 2021
.microsoft.com	MC1	GUID=2b3c3c7994b844d5afcc9f9a31bec967&HASH=2b3c&LV=20...	8 de junio de 2021



Advocacy and impacts



- Various meetings with Government and Mayor House (non public report sent first)
- Authentication vulnerabilities has been resolved in two apps (Coronapp, Cali) and one websites (MedellinmeCuida)
- HTTPS has been implemented in CoronApp and is beeing implemented in Bogota Cuidadora
- data collection and permissions has been limitedated in CoronApp
- However, privacy and digital security need still to be improved, a lot....



¡Thanks!

