

# **COVID-1984: Propaganda and Surveillance during a Pandemic**

## **[Argentina, 2020] [English | Spanish]**

### **ENGLISH**

#### **ABSTRACT**

The official political propaganda and digital surveillance in Argentina are not new. However, in the last fifteen years, both phenomena have adopted in their favor a new technological approach worthy of study [1], with the emergence of companies dedicated to manufacturing online trends [22]; cyber militancy groups aimed at setting up debates, responding to them or denouncing rival trends in a coordinated way (forming a propaganda apparatus); the project to establish an exclusive social network for pro-government and “against the establishment” militants (sponsored by the Government itself) [20]; the rise of state digital surveillance after the implementation of a Cyber Patrol Protocol, and the permanent monitoring of citizens through a mandatory (by law) mobile government application during the COVID-19 Pandemic.

This work aims not only to review the previous events, but also to detail the two greatest milestones of political propaganda and digital surveillance in Argentina today: the political propaganda apparatus on social networks and the digital privacy abuses caused by the government application CUIDAR-COVID19 ([ar.gob.coronavirus](https://ar.gob.coronavirus)).

For the first case, a fictitious account (sock puppet) will be infiltrated within the propaganda apparatus on social networks to achieve a detailed technical dissection of its entire operation (including its interventions and actors). Our own cyber intelligence tool, Venator.lua, will be used to obtain and process data.

The following section will be devoted to the study of privacy abuses caused by the mandatory government application CUIDAR-COVID19, reverse engineering it and analyzing its source code.

#### **KEYWORDS**

political propaganda, propaganda apparatus, propaganda machine, trolls, viral content, twitter, social networks, lua, venator, infodemics, Argentina

#### **ABOUT THE AUTHORS**

Mauro Cáseres ([mauroeldritch](https://mauroeldritch.com)) is an Argentine hacker and speaker. He spoke at several specialized conferences, including DEF CON Las Vegas, DevFest Siberia, DC 7831 Nizhny Novgorod, DragonJAR Colombia, P0SCon Iran and Roadsec Brazil.

---

# COVID-1984: El aparato de propaganda estatal durante una pandemia

## [Argentina, 2020] [Inglés | Español]

### ESPAÑOL

#### ABSTRACT

La propaganda política oficialista y la vigilancia digital en Argentina no son una novedad. Sin embargo en los últimos quince años, ambos fenómenos adoptaron en su favor un nuevo enfoque tecnológico digno de estudio [1], con el surgimiento de compañías dedicadas a *fabricar tendencias en línea* [22]; grupos de militancia *cibernética* destinados a implantar debates, responder a los mismos o denunciar tendencias rivales de forma coordinada; el proyecto para establecer una contra-red social exclusiva para militantes oficialistas y “*contra el establishment*” (auspiciada por el propio Gobierno)[20]; y el auge de la vigilancia digital estatal tras la implementación de un Protocolo de Ciberpatrullaje, y el seguimiento permanente de la ciudadanía a través de una aplicación móvil gubernamental de uso obligatorio durante la Pandemia de COVID-19.

Este trabajo apunta no sólo a reseñar los anteriores eventos, sino también a detallar los dos mayores hitos de la propaganda política y la vigilancia digital en Argentina a la actualidad: el aparato de propaganda política en redes sociales y los abusos a la privacidad digital causados por la aplicación gubernamental CUIDAR-COVID19 (*ar.gob.coronavirus*).

Para el primer caso, se infiltrará una cuenta ficticia (*sock puppet*) dentro del aparato de propaganda en redes sociales para lograr una disección técnica detallada de toda su operación (incluyendo sus intervenciones y actores). Se utilizará una herramienta de ciber inteligencia propia, *Venator.lua*, para la obtención y procesamiento de datos.

La siguiente sección estará dedicada al estudio de los abusos de privacidad causados por la aplicación gubernamental obligatoria CUIDAR-COVID19, realizando ingeniería inversa sobre la misma y analizando su código fuente.

#### PALABRAS CLAVE

*propaganda política, aparato de propaganda, máquina de propaganda, trolls, contenido viral, twitter, redes sociales, lua, venator, infodemia, argentina*

#### ACERCA DEL AUTOR

Mauro Cáseres (mauroeldritch) es un hacker y orador argentino. Ha disertado en varias conferencias especializadas, incluyendo DEF CON Las Vegas, DevFest Siberia, DC 7831 Nizhny Nóvgorod, DragonJAR Colombia, P0SCon Irán y Roadsec Brasil.

#### BREVE INTRODUCCIÓN A LA PROPAGANDA POLÍTICA EN REDES SOCIALES

La propaganda política oficialista en Argentina no es una novedad. Desde los comienzos del gobierno de Néstor Kirchner (FpV, 2003) se ha notado en medios y foros abiertos a la opinión la presencia permanente de usuarios comentando a favor del mismo. Dichos comentaristas compartían diversos rasgos que permitían establecer a simple vista un patrón: Carecían de foto de perfil (avatar), empleaban términos y frases en común (tema que será tratado en detalle posteriormente), y sus comentarios brindaban una versión en común para replicar al tema principal de la nota, especialmente si el foco era criticar una medida gubernamental.

En consecuencia a este comportamiento reiterativo y de enjambre, otros foristas dedujeron que estos usuarios respondían a una organización dedicada a la *formación de tendencias y opiniones a favor del gobierno Kirchnerista* (hecho que no fue blanqueado públicamente hasta años más tarde [14]). Bautizaron a estos *formadores de opinión* como “Cyber-Ks”, neologismo muy difundido a través de los años, e incluso immortalizado en la literatura nacional [12].

La actividad de los *Cyber-Ks* continuó intacta durante los siguientes dos gobiernos Kirchneristas, a cargo de la Presidente Cristina Fernández de Kirchner (FpV, 2007-2015) [4]. A este período se le suman peculiares casos de censura consumada en la prensa local [18], incluso contra funcionarios de su propio gobierno [19] y contra una serie internacional que osó deslizar un chiste sobre la figura del General Perón [17], lo cual sólo fue fructífero en generar polémica y rechazo como resultado.

En el transcurso de su gestión un grupo de militantes desarrolló un clon de la popular red social *Facebook*, llamada *FacePopular* [20][21][23] orientada a militantes y “contra el establishment”. En dicha red tenían lugar debates políticos oficialistas, donde surgirían discursos y tendencias en común que sus usuarios replicarían en otras redes. Fue un prototipo de lo que ocurriría en Twitter años más tarde.

La posterior gestión, a cargo de Cambiemos con Mauricio Macri como Presidente, no estuvo exenta de este comportamiento, viéndose involucrada en un escándalo sobre uso de robots (o cuentas zombie) durante la campaña electoral de 2019 [13][17], e incluso involucrando a la controversial compañía Cambridge Analytica en una campaña sucia contra el Kirchnerismo, reconocida por el propio CEO de la compañía ante la Justicia [3].

TECNO

# "¡Satisface a Mauricio!", "caricia significativa" y otras frases insólitas viralizadas en Twitter abrieron un debate sobre los bots en campaña

El oficialismo había convocado a sus seguidores a instalar una tendencia en redes sociales a favor de Macri, pero todo terminó en un gran sainete que demostró cómo se pueden alterar las conversaciones genuinas



Por **Desirée Jaimovich** | 9 de agosto de 2019  
djaimovich@infobae.com

[Compartir en Facebook](#)

[Compartir en Twitter](#)

- Lavonne Smythorsmith** @LavonneSmythor1 · 8 ago.  
La continuación con el FMI ayuda a a obtener liquidación de sus obligaciones financieras bajo el mismo gobierno federal. #YoVotoMM

1
- Lavonne Smythorsmith** @LavonneSmythor1 · 8 ago.  
¡Satisface a Mauricio, no te relajes! Te elijo! ¡Caricia significativa proveniente de Hurlingham! #YoVotoMM

251 1,1 K 2,9 K
- Lavonne Smythorsmith** @LavonneSmythor1 · 8 ago.  
Los arreglos de las autoridades preparadas del Sr. Macri con el FMI ayudaron a en una dispensación más rápida del informe de crédito.

1

MÁS LEÍDAS

- 1 Coronavirus en la Argentina: confirmaron 474 casos nuevos y es el día de más contagios desde que comenzó la pandemia
- 2 Alberto Fernández acordó con Kicillof y Rodríguez Larreta una estrategia común para el transporte público del AMBA en la nueva etapa de cuarentena
- 3 Bono de Anses: arranca en junio el pago de la segunda tanda del IFE
- 4 "Soy un milagro de Dios": el aterrador relato de la mujer que traicionó al Chapo Guzmán
- 5 El insólito método para traficar drogas del Chino Antrax, el taquero que llegó a la cima del Cábel de Sinaloa

*Infobae: Bots utilizados para la campaña de Cambiemos, escribiendo en Español con notables errores. Edición del 9 de Agosto de 2019.*

Durante el comienzo de este período de gobierno, el Kirchnerismo como oposición tomó un rol más sutil en cuanto a la difusión de propaganda, hecho que quedó demostrado en 2016 tras la filtración de un "manual de micro militancia", donde se detallan pautas para sostener la imagen de su anterior gobierno (esta vez, sin el sustento económico ni político) [16][25].

## ARGENTINA

## El insólito manual de "micro militancia" K para resistir al Gobierno

El instructivo, que se viralizó en las redes sociales, busca "despertar conciencia" contra Mauricio Macri. Incluye 10 "técnicas", desde intervenir diarios en bares a realizar "actings" en supermercados

14 de enero de 2016

Compartir en Facebook

Compartir en Twitter

### TECNICAS DE RESISTENCIA ACTIVA-MICROMILITANCIA



162

Un pintoresco folleto kirchnerista con título "Técnicas de resistencia activa - Micromilitancia" empezó a circular masivamente por las redes sociales. Se trata de un decálogo con propuestas para movilizar pequeñas acciones contra el gobierno de Mauricio Macri al que define "de corte neoliberal" y nosea "un blindaje de medios de información

## MÁS LEÍDAS

- 1 Coronavirus en la Argentina: confirmaron 474 casos nuevos y es el día de más contagios desde que comenzó la pandemia
- 2 Alberto Fernández acordó con Kicillof y Rodríguez Larreta una estrategia común para el transporte público del AMBA en la nueva etapa de cuarentena
- 3 Bono de Anses: arranca en junio el pago de la segunda tanda del IFE
- 4 "Soy un milagro de Dios": el aterrador relato de la mujer que traicionó al Chapo Guzmán
- 5 El insólito método para traficar drogas del Chino Antrax, el taquero que llegó a la cima del Cártel de Sinaloa

THE NEW YORK TIMES

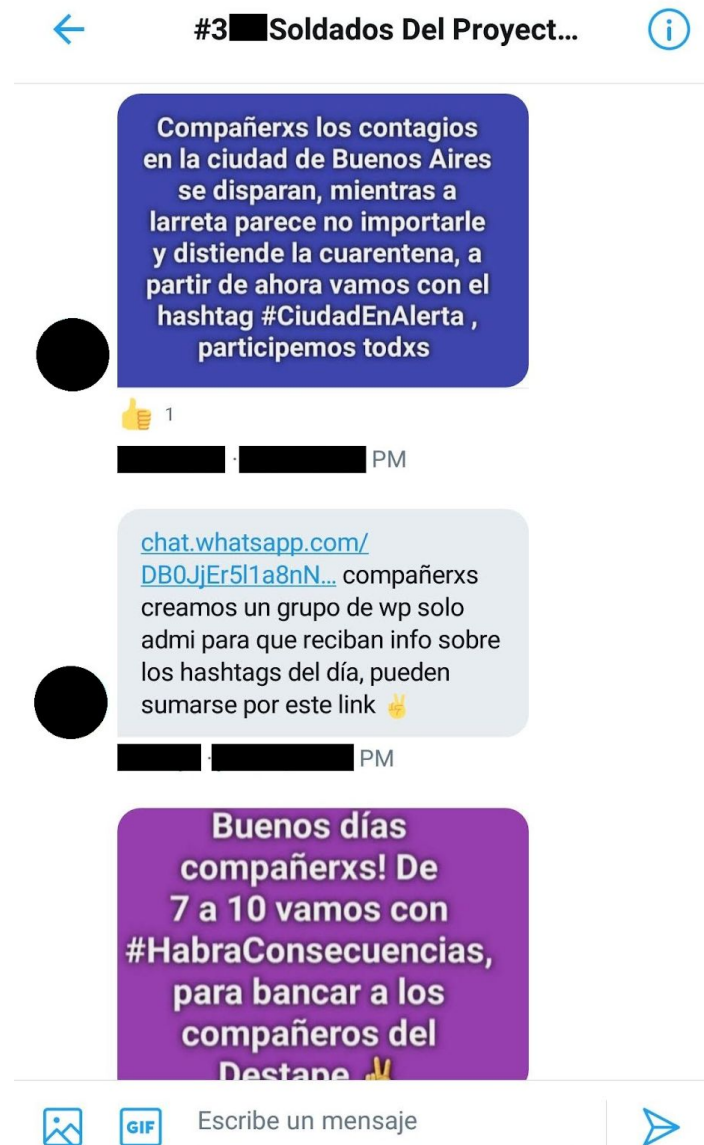
*Infobae: Manual de micro militancia. Edición del 14 de Enero de 2016.*

A comienzos del actual gobierno a cargo del Presidente Alberto Fernández (FdT), se hicieron públicos los detalles acerca de los "Cyber-Ks" que desde 2003 hasta entonces eran desconocidos. Toda su estructura fue explicada por su "líder", el Ingeniero Ariel Garbarz a la Revista Noticias [14][15], confirmando definitivamente lo que hasta el momento era una especulación. Es a partir de este momento donde se establece el foco del presente trabajo.

### BREVE ANÁLISIS DE INTERVENCIONES PROPAGANDÍSTICAS EN TWITTER

Las intervenciones propagandísticas en Twitter responden como es habitual, a un colectivo organizado de *cibermilitantes* [14]. Liderados por *coordinadores*, los *cibermilitantes* se nuclean en grupos de WhatsApp y Twitter, donde reciben a diario uno o más *comunicados*, que constan de una breve reseña sobre un hecho político, económico y/o social reciente y un *hashtag* representativo de la situación, el cual deben viralizar para establecer una tendencia.

La viralización de este contenido se efectúa simplemente escribiendo (“*twitteando*”) dicho hashtag en tantas publicaciones como sea posible en una pequeña ventana de tiempo. Es así como unas pocas personas pueden *subir la temperatura* de un término dado y establecerse entre las primeras posiciones de las tendencias (“*trending topics*”) de forma repentina.



*Twitter: Grupo de difusión de propaganda oficialista donde se dictan las tendencias a viralizar. Nótese que también se comparte un enlace a un grupo de WhatsApp de las mismas características.*

Estos grupos se desenvuelven a grandes rasgos de tres formas: *formando* tendencias (viralizando contenido); *respondiendo* tendencias contrarias, ya sea unificando una versión de los hechos para replicar una publicación (“Nuestra economía está mal porque recibimos un país destruido por años de *neoliberalismo*”), o *polarizando* contenido para desvirtuar el

tema de la conversación (“Nuestra presidente tendrá cuentas en Seychelles, pero ¿qué me dicen de las cuentas offshore de [el candidato opositor, Mauricio] Macri?”); y en tercer lugar, *bajando* (censurando) cuentas, hilos y tendencias opositoras (denunciando una tendencia opositora bajo el rótulo de *discurso de odio, ser perjudicial o cometer abusos contra un grupo de personas por su pensamiento político*).

Es entendible para el lector promedio pensar que no existe *dolo* en el hecho de viralizar una tendencia política, así como no lo habría por ejemplo, al momento de viralizar el nombre de un equipo de fútbol tras ganar una final, o el de una compañía de videojuegos que está regalando uno de sus mejores títulos como estrategia de marketing. Sin embargo, Twitter terminantemente especifica lo contrario y toma acción directa contra este tipo de comportamiento [2].

En cuanto a las denuncias masivas para *bajar* contenido, no es el único intento de censura que se ha intentado materializar en las redes sociales, como se analizará en la próxima sección.

## **ESFUERZOS POLÍTICOS POR LIMITAR LA LIBERTAD DE EXPRESIÓN EN REDES SOCIALES**

Los esfuerzos políticos por limitar la libertad de expresión en medios digitales fueron ejecutados o sugeridos mayormente por el actual oficialismo (peronismo, justicialismo, kirchnerismo), aunque los datos fríos como los demostrados por el *Reporte de solicitudes gubernamentales de información sobre los usuarios* de Google INC demuestra que es una práctica extendida en todo el espectro político [C].

Estos esfuerzos no se limitan al actual gobierno (año 2020, Partido Frente de Todos - FdT) sino que sus primeros intentos pueden hallarse revisando desde su anterior gestión (particularmente en el año 2014, Partido Frente para la Victoria - FpV) cuando dos legisladores de la Provincia de Chaco, Beatriz Bogado y Rubén Guillón, propusieron una iniciativa para que los portales de internet sólo permitan comentar a personas registradas con nombre real, domicilio y número de Documento Nacional de Identidad. [7]



## Chaco: proponen que los usuarios que comentan en sitios web se identifiquen con su nombre real y DNI

Es una iniciativa de dos legisladores peronistas; también se pediría domicilio

23 de abril de 2014 • 20:28



Comentar  
(514)



Me gusta



Compartir

**L**os legisladores peronistas Beatriz Bogado y Rubén Guillón, propusieron una iniciativa en la provincia de Chaco para que los portales de Internet sólo dejen publicar comentarios a las personas que introduzcan todos sus datos, incluyendo nombre real, DNI, y domicilio.

Según el [Diario Chaco](#), la iniciativa prevé que "los portales de Internet que habiliten la introducción de comentarios en los sitios que poseen en la Red Informática Mundial (World Wide Web), deberán prever los mecanismos informáticos que fueren necesarios, a los efectos de que los emisores acrediten, previamente y de manera fehaciente, su identidad (nombre y apellido, documento nacional de identidad, domicilio real); la que deberá ser exhibida de manera inequívoca en el portal. En ningún caso podrán publicarse expresiones y/o comentarios en dichos sitios virtuales, sin previo cumplimiento de este requisito".

La norma también obligaría a los portales de Internet a anunciar la medida a sus usuarios de la siguiente forma: "Señor Usuario: Quedan bajo su exclusiva responsabilidad los comentarios que realice en el presente portal digital, debiendo utilizar el mismo de acuerdo a la normativa legal vigente".

De igual forma, la responsabilidad de los comentarios publicados por los

### RECOMENDADOS

Murió Natacha Durán, "chica Sofovich" y conductora de El Garage TV



Coronavirus: por qué el ejemplo de España muestra que el mundo necesitará nuevas cuarentenas



Coronavirus: Jair Bolsonaro, entre risas y chistes después del récord de más de mil muertes diarias en Brasil



Alejandro Fantino y los rumores de romance con Luciano Pereyra: "Es una historia de un romanticismo terrible"



### MÁS LEÍDAS DE SOCIEDAD



*La Nación. Editorial del 23 de Abril de 2014.*

En un contexto actual, el Senador Alfredo Luenzo (FdT) subió la apuesta proponiendo textualmente la *regulación pública y democrática* de las redes sociales [8][9]. Desde las mismas, respondieron con un masivo repudio.



## Un senador del Frente de Todos propone una "regulación pública y democrática" de las redes sociales



Un senador del Frente de Todos propone una "regulación pública y democrática" de las redes sociales Fuente: Archivo

### RECOMENDADOS

Murió Natacha Durán, "chica Sofovich" y conductora de El Garage TV



Coronavirus: por qué el ejemplo de España muestra que el mundo necesitará nuevas cuarentenas



Coronavirus: Jair Bolsonaro, entre risas y chistes después del récord de más de mil muertes diarias en Brasil



Alejandro Fantino y los rumores de romance con Luciano Pereyra: "Es una historia de un romanticismo terrible"



### MÁS LEÍDAS DE POLÍTICA



*La Nación. Editorial del 22 de Abril de 2020.*



*Twitter personal del Senador Luenzo. 18 de Abril de 2020.*

Un día después de efectuadas estas declaraciones, se da a conocer el *Protocolo de Ciberpatrullaje* de la Ministra de Seguridad de la Nación, Sabina Fréderic (FdT)[10]. Nuevamente, esto conllevó a un enérgico repudio en las redes.

## CORONAVIRUS

# Los detalles del protocolo de “ciberpatrullaje” que impulsa el Gobierno: qué busca regular y cuáles son los puntos más cuestionados

La ministra de Seguridad, Sabina Frederic, presentó el primer borrador ante organismos de derechos humanos, el sector más crítico



Por **Juan Piscetta**

19 de abril de 2020

[jpiscetta@infobae.com](mailto:jpiscetta@infobae.com)

Compartir en Facebook

Compartir en Twitter



## MÁS LEÍDAS

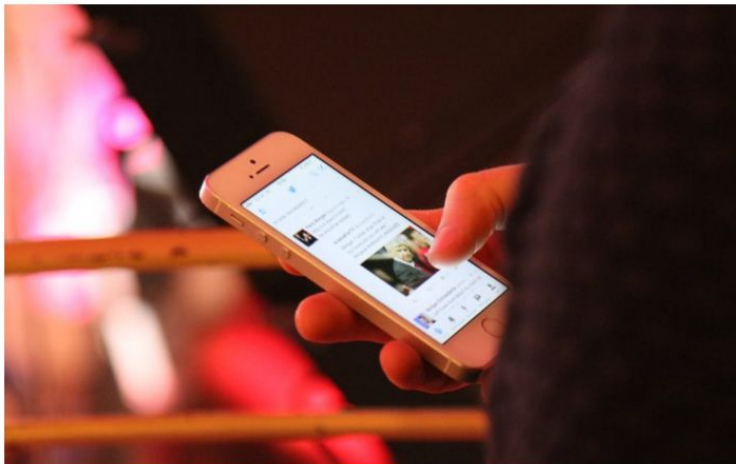
- 1 Bono de Anses: arranca en junio el pago de la segunda tanda del IFE 
- 2 La verdad sobre la muerte de la conductora y actriz Natacha Durán: “Ella siempre tuvo la intuición de que partiría joven” 
- 3 El insólito método para traficar drogas del Chino Antrax, el taquero que llegó a la cima del Cártel de Sinaloa 
- 4 Sospechas de engaño en las redes: famosas, envueltas en una polémica promoción de una máquina facial 
- 5 La espeluznante historia del “exitoso médico” que asesinó a su esposa, a sus hijos y a sus padres sin piedad 

*Infobae. Editorial del 19 de Abril de 2020.*

Tan sólo dos días después, dicho *protocolo* dio su primer “caso positivo”, resultando en un arresto a un ciudadano debido a un mensaje publicado en su cuenta personal de la plataforma Twitter, y continuó con una serie de 20 allanamientos por la misma causa [11].

## DETENIDO POR TUITEAR: EL CIBERPATRULLAJE CONTRA LOS DERECHOS HUMANOS EN ARGENTINA

Abr 21, 2020 | Libertad de expresión



Sabina Frederic, ministra de Seguridad del gobierno federal de Argentina, compareció el 7 de abril ante la Comisión de Seguridad Interior de la Cámara de Diputados. En su intervención, declaró que tanto las fuerzas de seguridad pública civiles como la Gendarmería Nacional –organismo de naturaleza militar con funciones mixtas– realizaban “ciberpatrullaje” en las redes sociales para evaluar el “humor social” de las personas y determinar si había “incitación al odio” en ellas, pero que no se trataba de una medida de inteligencia.

*Red de Defensa de los Derechos Digitales: Editorial del 21 de Abril de 2020.*

### ENTRADAS RECIENTES

La industria del reconocimiento facial quiere identificar a las personas que utilicen cubrebocas  
Zoom está rastreando videollamadas con contenido sexual

Necesidad de salvaguardar la libertad de expresión, incluyendo el derecho a videogravar, durante la pandemia del COVID-19 en América Latina

NSO trató de vender su tecnología a policías locales en EE.UU.

Medio chileno publica mapas con la ubicación de personas diagnosticadas con Covid-19

Algunos días después y a tono de las medidas de cuarentena obligatoria, el Gobierno propuso - y luego dio marcha atrás con la medida - regular el tránsito de ciudadanos en la ciudad bloqueando unilateralmente el uso de sus tarjetas de transporte público (SUBE) de determinados sectores de la población [26], en otro claro ejemplo de medidas políticas abusivas impuestas mediante el uso de sistemas tecnológicos gubernamentales.

Ambas medidas (el ciberpatrullaje y el bloqueo de tarjetas) fueron ampliamente defendidas en redes sociales por miembros del aparato de propaganda antes mencionado, quienes sostuvieron que dichas medidas no violaban la privacidad de los usuarios, sino que estaban orientadas a “protegerlos”.

### INFILTRACIÓN EN EL APARATO DE PROPAGANDA POLÍTICA NACIONAL

Para la infiltración en el aparato de propaganda política fue necesaria la creación de una cuenta de Twitter ficticia (*sock puppet*). Para la confección de la misma se tuvo en cuenta el patrón de configuración fácilmente observable de las cuentas dedicadas a difundir propaganda pro-gobierno: Foto de perfil de la dupla presidencial Alberto y Cristina Fernández, foto de portada de la entonces Presidente Cristina Fernández en su acto en el

Estadio Vélez Sarsfield, descripción del perfil con frases previamente estudiadas en otros perfiles como “*Siempre del lado correcto de la mecha*”, “*La vamos a redistribuir*” (las riquezas “concentradas”), “*Dijo chiques, y me conquistó*” (sic), en alusión al lenguaje inclusivo empleado por el primer mandatario en actos públicos, y el uso de *emojis* específicos adoptados por simpatizantes de este movimiento: el corazón verde (simbolizando la militancia a favor de la campaña “Aborto Legal, Seguro y Gratuito”) y la V de la victoria, gesto utilizado por los peronistas.

Esta cuenta fue creada a fines de Abril y se mantuvo sin actividad hasta Mayo para tener al menos un mes de antigüedad antes de comenzar a operar.

El acercamiento al aparato de propaganda fue planteado en fases: **la primera** incurrió en la observación e identificación de recursos de valor: cuentas pro-gobierno *populares* que incurran en la viralización de contenido; frases en común; nubes de palabras (términos de mayor *temperatura*); y comportamiento general (particularmente las reacciones hacia comentarios adversos de la oposición y el manejo de dicha situación). Esta reconocimiento primario permitiría la creación de piezas de inteligencia que contribuirían al desarrollo de la cuenta ficticia y con él, mejorarían las posibilidades no sólo de ser reclutada dentro del aparato propagandístico, sino de que pueda permanecer desapercibida una vez dentro el tiempo suficiente para estudiarlo.

**La segunda etapa** incurrió en seguir a 50 cuentas oficialistas *populares* en el primer día, y publicar diariamente un mensaje utilizando las frases comunes estudiadas en la etapa anterior, en combinación con hashtags oficialistas y en lo posible, utilizando los términos más reiterados en la nube de palabras confeccionada previamente. Algunos de estos términos fueron: *neoliberalismo*, *neocolonialismo*, *gorilas* (término despectivo para referirse a opositores al peronismo), *bolsonazi* (término despectivo para referirse al Presidente de Brasil Jair Bolsonaro), *piraña* (Término despectivo para referirse al Presidente de Chile Sebastián Piñera), *globerto* (Término despectivo para referirse a votantes de Cambiemos), *globoludo* (Ídem anterior), *chiques* (“Chicos” en lenguaje inclusivo), *Magneto* (CEO de Grupo Clarín). La idea concreta de esta etapa fue la de generar una actividad inicial y ganar un primer lote de seguidores para comenzar a generar confianza en la cuenta ficticia. Se consiguieron veinte seguidores en el primer día.

**La tercera etapa** consistía en obtener un lote mayor de seguidores participando activamente de “listas de seguidores”, hilos de Twitter donde un usuario que desea nuevos seguidores debe marcar como favorito el primer mensaje y *retwittearlo*, para luego seguir a todos los que hayan hecho lo mismo mirando las listas de “Favoritos” y “Retweets” respectivamente. Posteriormente otros usuarios harían lo mismo, encontrando la cuenta ficticia en dichas listas y siguiéndola. Asimismo, se consigna que todo usuario que sea “seguido” por otro debe recíprocamente seguirlo también, generando una cadena. La gran cantidad de usuarios en estas listas deja a nuestra cuenta ficticia con una discreta impunidad, lo que evita posibles desconfianzas al seguir a usuarios individuales sin interacción previa, ya que se trata de un proceso casi “automático”. Este paso generó unos ochenta seguidores nuevos en tres horas y media.

**La cuarta fase** conllevaba no menos que el reclutamiento. Esto demoró apenas tres días, cuando uno de los coordinadores mencionados en la entrevista a Ariel Garbarz [14] envió un mensaje a la cuenta ficticia, invitándola a formar parte de un grupo para “*compartir hashtags*”. La invitación fue aceptada y unas horas después la cuenta formaba parte de un

grupo numerado. Dicho número de identificación indicaba que había al menos, unos 350 grupos de propaganda anteriores, en actividad.

Como dato curioso, este mismo usuario volvió a reclutar a la cuenta ficticia diez días después, desde otra de sus cuentas personales. Es probable que haya “desconocido” y “redescubierto” la cuenta ficticia navegando entre hashtags de propaganda. La invitación fue aceptada, y la cuenta ficticia fue agregada a un nuevo grupo numerado.

Tomando la diferencia de número de identificación entre el primer y segundo grupo a los que el usuario ficticio fue invitado, fue posible tomar un patrón de crecimiento del aparato de propaganda: cada grupo de Twitter puede tener hasta cincuenta usuarios, y entre el primer y segundo grupo existe una diferencia de seis dígitos, es decir, seis grupos nuevos con cincuenta usuarios cada uno. Esto resulta en **aproximadamente trescientos usuarios nuevos en diez días, al servicio de la difusión de propaganda.**

**La quinta fase** recayó en la participación sistemática de cada consigna propagandística enviada al grupo por los coordinadores. Esto garantizaba la permanencia en el grupo el suficiente tiempo para realizar los estudios necesarios, detallados más adelante.





*Twitter: Primer invitación de un Coordinador del aparato de propaganda.*



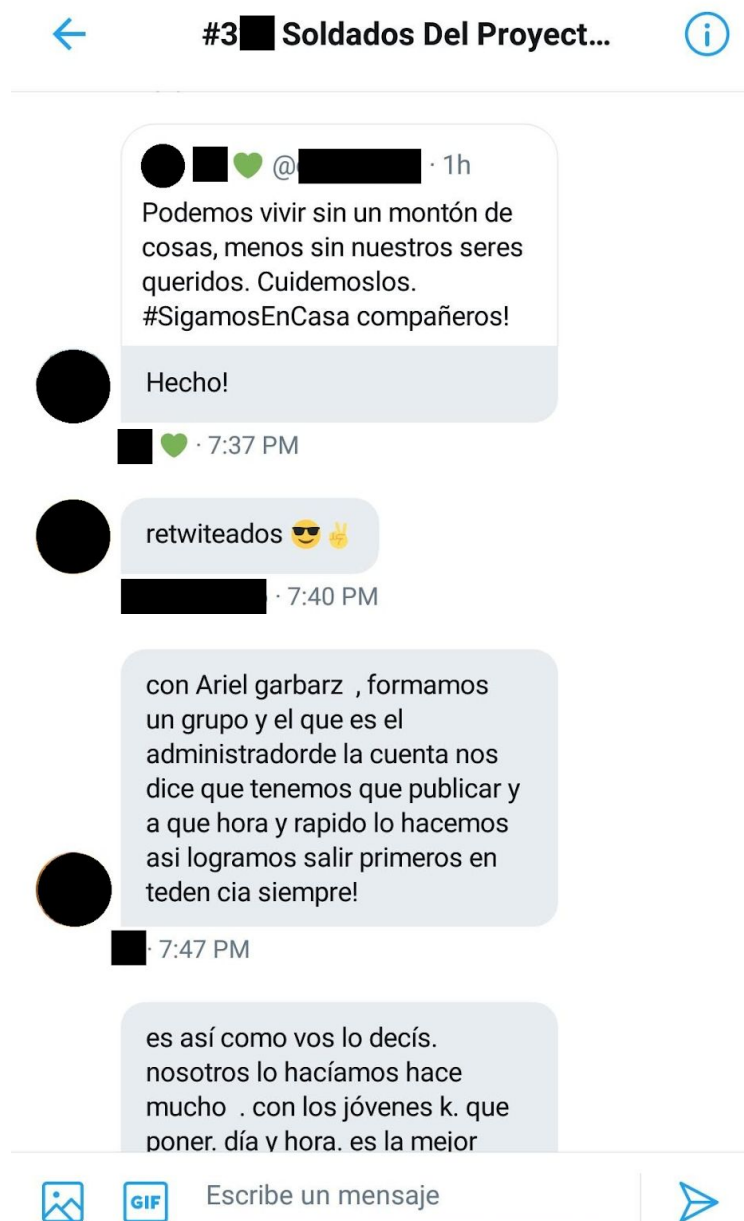
*Twitter: Segunda invitación del anterior Coordinador al aparato de propaganda.*

## DISECCIÓN DE UNA INTERVENCIÓN PROPAGANDÍSTICA EN REDES SOCIALES

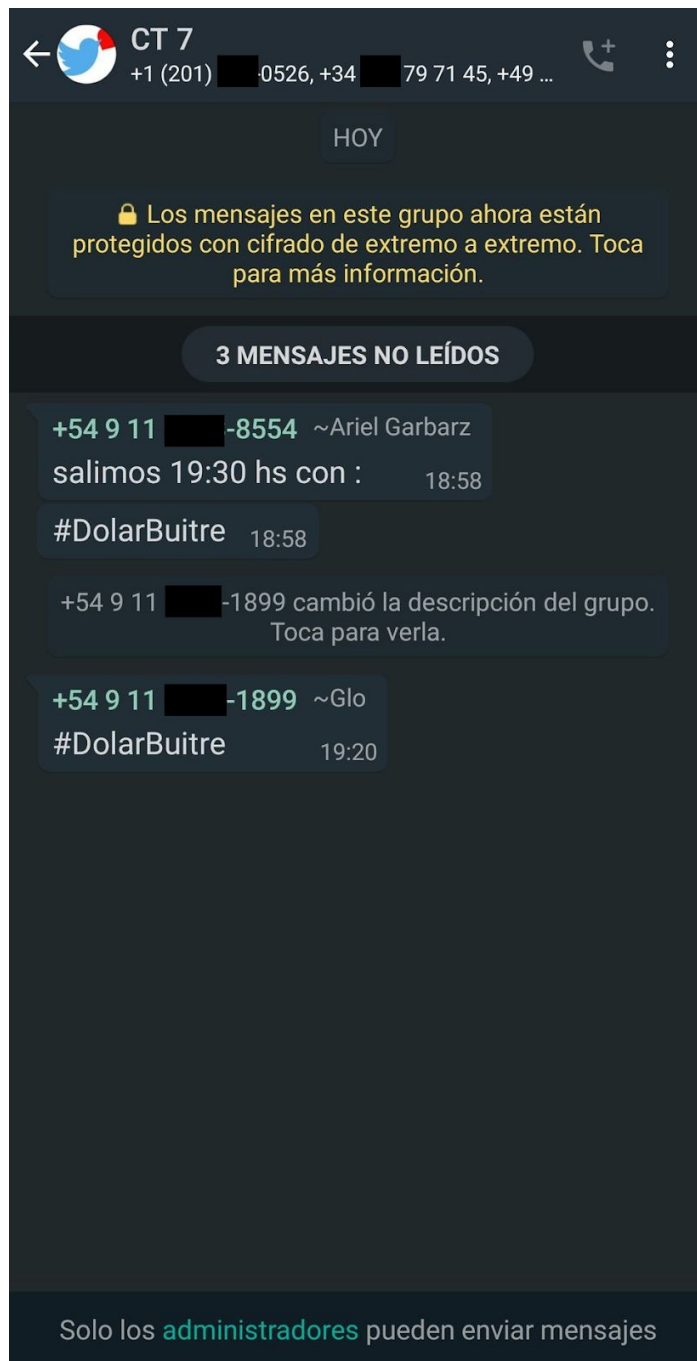
Las intervenciones propagandísticas respetan un mecanismo muy simple: El *Líder* y los *Coordinadores* discuten un hashtag para hacerlo tendencia; los *Coordinadores* luego lo comunican a cada uno de sus grupos de *Militantes* vía WhatsApp (grupo unidireccional) o vía Twitter (grupo multidireccional). Estos *Militantes* son la base de la pirámide, y son quienes masifican (viralizan) dicho hashtag.



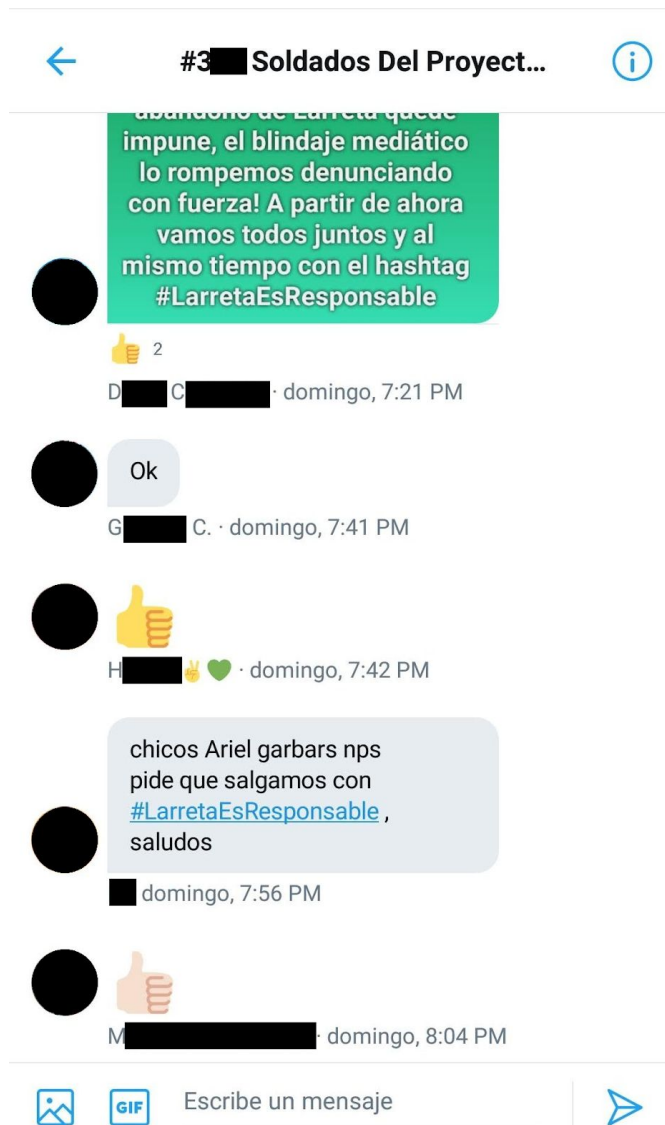
Como se ha mencionado anteriormente, cuando un término sube de *temperatura* (cantidad de menciones) notablemente en un corto lapso de tiempo, se convierte fácilmente en tendencia. Si dicha tendencia es provocativa genera respuestas, lo que sólo sirve a su propósito original: seguir generando menciones y “movimiento” en torno a dicho término. Más se menciona un término, independientemente si es a favor o en contra; en un relato real, manipulado o falso; más reiteraciones contabilizará el algoritmo de la red social de forma fría e indefectible. A esta sobreabundancia de información se le conoce como *infodemia*.



Twitter: Mención de Ariel Garbarz [14] y los grupos de WhatsApp.



*WhatsApp: Orden de comienzo de una intervención propagandística por Ariel Garbarz y otro Líder ("Glo"). Nótese la presencia de miembros internacionales (+1, Estados Unidos; +34, España; +49, Alemania).*



*Twitter: Nuevamente un coordinador envía un hashtag atacando al Jefe de Gobierno de la Ciudad Buenos Aires. Debajo, otro militante repite la consigna enviado por el Líder, Ariel Garbarz.*

Este proceso es rústico pero eficaz, ya que su impacto es públicamente visible **a diario en Twitter**. Asimismo, existen sistemas en línea dedicados a recopilar un histórico de tendencias minuto a minuto, donde puede apreciarse fácilmente y en tiempo real la expansión de la infodemia [26].

## DISECCIÓN DE UN APARATO PROPAGANDÍSTICO EN REDES SOCIALES

Para el análisis de la red propagandística se utilizaron herramientas de terceros como Botometer [D], y la librería Twitter para Ruby [E], para una identificación básica sobre el comportamiento de cuentas específicas. Sin embargo, no existen - al menos en el dominio

público - herramientas propicias para lograr un análisis de mayor complejidad, por lo cual se decidió crear Venator.lua, una aplicación destinada al análisis de comportamientos propagandísticos (explicada en detalle más adelante).

```
fish /home/plaguedoktor/Projects/COVID-1984
Archivo Editar Ver Buscar Terminal Ayuda
Venator.lua
@mauroeldritch (plaguedoktor) - 2020

[!] Data for user: M 0144529
[*] Created at: Mon Aug 12 16:00:25 +0000 2019
[!] Default Profile: true
[*] Default Image: false
[!] Following Count: 117
[!] Followers Count: 19
[*] Tweets Count: 556
[?] Verified Profile: false

[!] Final Score: 60/100.

[!] Username contains many numbers. This may indicate a default username given by the platform.
[!] This account has default profile settings enabled.
[!] This account has fewer Followers than Followed.
[!] This account has less than 50 Followers.
[?] This account is not verified. This does not affect the Final Score.
✓ COVID-1984 (master) x
```

*Venator: Análisis de una cuenta individual en busca de rasgos sospechosos.*

```
fish /home/plaguedoktor/Projects/COVID-1984
Archivo Editar Ver Buscar Terminal Ayuda
Venator.lua
@mauroeldritch (plaguedoktor) - 2020

[*] @gui aneg1 (25|118) [RTs: -0] [Fav: -0]: @maquialifracco Perón, y con eso se acomoda el resto!
[*] @jhe peron (335|244) [RTs: -0] [Fav: -0]: @jpcmpdperteito
[*] @gol ueen (664|211) [RTs: 1057] [Fav: -0]: RT @ChauOperetaK: ¿Cuántos somos los que creemos que SIN PERÓN, muy probablemente hoy Argentina sería potencia mundial? 🇦🇷
[*] @ma bouso (386|655) [RTs: 6] [Fav: -0]: RT @Alfredobarrio: Los K proponiendo que Macri y banda vayan ya presos"
y el principio de presunción de inocencia?
y la innecesariedad d...
[*] @j peron (335|244) [RTs: -0] [Fav: -0]: @jordannalopes15
[*] @Car lgres4 (78|204) [RTs: -0] [Fav: -0]: Muy complejo, sin Perón o somos potencia o somos una dictadura comunista. Históricamente si pudiera eliminar a uno... https://t.co/FNbv73DTc0
[*] @RI rec2 (14|24) [RTs: 1057] [Fav: -0]: RT @ChauOperetaK: ¿Cuántos somos los que creemos que SIN PERÓN, muy probablemente hoy Argentina sería potencia mundial? 🇦🇷
[*] @RHO aaf (335|278) [RTs: 1057] [Fav: -0]: RT @ChauOperetaK: ¿Cuántos somos los que creemos que SIN PERÓN, muy probablemente hoy Argentina sería potencia mundial? 🇦🇷
[*] @Ew rerrera (554|335) [RTs: 12] [Fav: -0]: RT @Gus Sastre: Recibimos a los vecinos del barrio Presidente Perón y dialogamos sobre la obra de extensión de energía eléctrica que consta...
[*] @T iKuka (145|309) [RTs: -0] [Fav: -0]: @tanoproductor Mi viejo, LA VIDA. Y PERÓN, yo escucho un audio diferente de Perón como mínimo cada semana, y lo voy... https://t.co/Xu5x4IBBME
✓ COVID-1984 (master) x
```

*Venator: Análisis de la tendencia “Perón” en tiempo real para identificar seguidores y detractores.*

```
fish /home/plaguedoktor/Projects/COVID-1984
Archivo Editar Ver Buscar Terminal Ayuda

t": {"1"}, {"hashtag": "reachelrusch", "count": "1"}, {"hashtag": "reginaszellesok", "count": "1"}, {"hashtag": "reiscarolina", "count": "1"}, {"hashtag": "relias23", "count": "2"}, {"hashtag": "respitforlali", "count": "1"}, {"hashtag": "ricalfonsin", "count": "1"}, {"hashtag": "ricfandino", "count": "1"}, {"hashtag": "riesgopaisok", "count": "1"}, {"hashtag": "riggshogwarts", "count": "1"}, {"hashtag": "rimaesbe", "count": "1"}, {"hashtag": "rinconet", "count": "1"}, {"hashtag": "ringskoo", "count": "1"}, {"hashtag": "robertojarias", "count": "1"}, {"hashtag": "robivillarruel", "count": "1"}, {"hashtag": "rociocarrizo", "count": "1"}, {"hashtag": "romagnoliclau", "count": "1"}, {"hashtag": "romancestoess", "count": "1"}, {"hashtag": "rosariovallab", "count": "2"}, {"hashtag": "salvachalo", "count": "1"}, {"hashtag": "sandrab cba", "count": "2"}, {"hashtag": "santil0243570", "count": "1"}, {"hashtag": "santicafiero", "count": "1"}, {"hashtag": "santisiri", "count": "1"}, {"hashtag": "saraplaquin", "count": "1"}, {"hashtag": "sastres 5", "count": "1"}, {"hashtag": "secsagenaria", "count": "2"}, {"hashtag": "selenaeuphoria", "count": "3"}, {"hashtag": "selvairis", "count": "1"}, {"hashtag": "sergiogcasas", "count": "1"}, {"hashtag": "sergioserrichio", "count": "2"}, {"hashtag": "sespiasse", "count": "1"}, {"hashtag": "sil npl", "count": "1"}, {"hashtag": "sil codoni", "count": "1"}, {"hashtag": "silvia cuc", "count": "2"}, {"hashtag": "silviaiomini", "count": "1"}, {"hashtag": "silviapiazzi", "count": "1"}, {"hashtag": "silvitasalinas", "count": "1"}, {"hashtag": "slythrnobrien", "count": "1"}, {"hashtag": "sofiacaram", "count": "1"}, {"hashtag": "sol despeinada", "count": "1"}, {"hashtag": "sol lopezok", "count": "1"}, {"hashtag": "sosacm", "count": "2"}, {"hashtag": "stoessxmernes", "count": "2"}, {"hashtag": "suipachero", "count": "1"}, {"hashtag": "surtidodebaires", "count": "1"}, {"hashtag": "sweetlizzie2", "count": "1"}, {"hashtag": "tampocolapavada", "count": "1"}, {"hashtag": "tellyquen", "count": "1"}, {"hashtag": "tenonblas", "count": "1"}, {"hashtag": "terebe06", "count": "1"}, {"hashtag": "thanksemilia", "count": "1"}, {"hashtag": "theinspector 5", "count": "1"}, {"hashtag": "thingsfortini", "count": "1"}, {"hashtag": "tinipetera", "count": "1"}, {"hashtag": "tinvalente22", "count": "1"}, {"hashtag": "todoeskk", "count": "3"}, {"hashtag": "tomimendec", "count": "1"}, {"hashtag": "torcho53", "count": "1"}, {"hashtag": "turkinga63", "count": "2"}, {"hashtag": "twama derna", "count": "1"}, {"hashtag": "unalettradadice", "count": "1"}, {"hashtag": "valenbeiguel", "count": "1"}, {"hashtag": "valenlottero", "count": "1"}, {"hashtag": "valenrr04", "count": "1"}, {"hashtag": "valmereres", "count": "1"}, {"hashtag": "veoenfotos", "count": "1"}, {"hashtag": "veronixe", "count": "1"}, {"hashtag": "vivicentlucas", "count": "1"}, {"hashtag": "volviendosiempr", "count": "1"}, {"hashtag": "walterfernandlm", "count": "1"}, {"hashtag": "williamhsby", "count": "1"}, {"hashtag": "winogradvictor", "count": "1"}, {"hashtag": "xestufita", "count": "1"}, {"hashtag": "yiy angcenter", "count": "1"}, {"hashtag": "yvaelterceroi", "count": "1"}, {"hashtag": "zamorajulio", "count": "1"}, {"hashtag": "zlotomcarcelo", "count": "1"}, {"hashtag": "zourabichvili_s", "count": "1"}]
✓ COVID-1984 (master) x
```

*Venator: Análisis de interacciones de una cuenta con sus seguidores.*

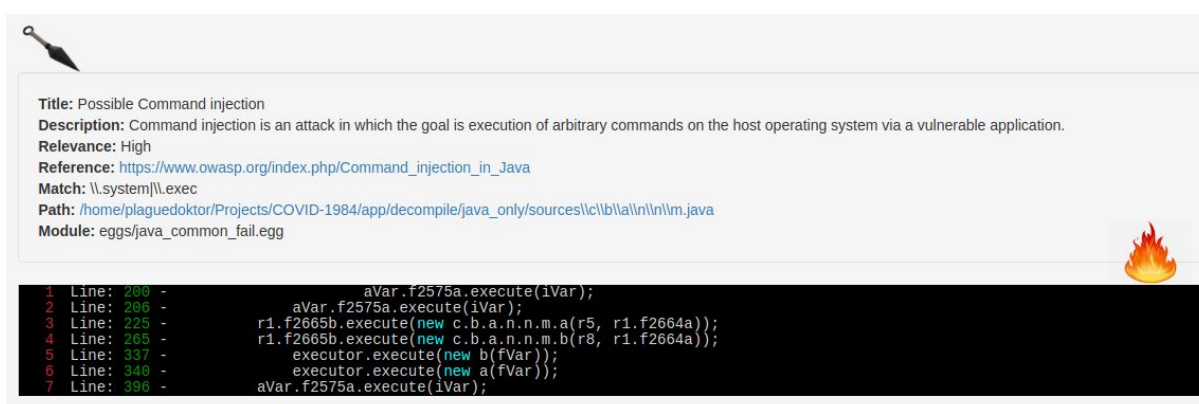
Los resultados de Venator en conjunto con la investigación manual se detallan a continuación:

- Existen más de **350 grupos de Twitter** con 50 integrantes cada uno.
- Descontando al coordinador de cada grupo (figura repetida en cada uno) quedarían 49 usuarios efectivos, lo que arroja un número final aproximado de **17.150 usuarios únicos a la fecha**.
- El patrón de crecimiento es de aproximadamente **30 usuarios nuevos por día**.
- El patrón de cuentas seguidas es el mismo: **99%** siguen al menos a un *Coordinador*, al Presidente Alberto Fernández, y a la Vicepresidente Cristina Fernández en simultáneo.
  - Un **90%** sigue al menos a la mitad de los Ministros.
- El porcentaje de acatamiento de los pedidos de difusión de propaganda es del **99%**. Aquellas cuentas inactivas son eliminadas por los administradores.

## AR.GOB.CORONAVIRUS: DISECCIÓN DE UNA APLICACIÓN GUBERNAMENTAL OBLIGATORIA

Durante la pandemia de COVID-19, el gobierno argentino decretó la cuarentena obligatoria, lanzando poco después una aplicación de uso obligatorio para todos aquellos que tuvieran permitido volver a la actividad [24]. Esto, en conjunto con distintas medidas políticas que tuvieron poca aprobación de la ciudadanía [26], despertó la polémica sobre la vigilancia digital, alegando que la aplicación podría violar la privacidad de los usuarios.

Tras un análisis profundo (con herramientas propias y de terceros) sobre el código desensamblado de la aplicación, es propicio decir que dicha polémica es justificada. A continuación, se detallan con capturas de pantalla las piezas de código más preocupantes.



*CodeWarrior: El código presenta varias oportunidades de ejecutar inyecciones de comandos.*





**Title:** Possible Command injection  
**Description:** Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application.  
**Relevance:** High  
**Reference:** [https://www.owasp.org/index.php/Command\\_injection\\_in\\_Java](https://www.owasp.org/index.php/Command_injection_in_Java)  
**Match:** \\system\\exec  
**Path:** /home/plaguedoktor/Projects/COVID-1984/app/decompile/java\_only/sources/com\\newrelic\\agent\\android\\instrumentation\\SQLiteInstrumentation.java  
**Module:** eggs/java\_common\_fail.egg



```
1 Line: 28 -      SQLiteDatabase.execSQL(str);
2 Line: 123 -      SQLiteDatabase.execSQL(str, objArr);
```

*CodeWarrior: El código presenta varias oportunidades de ejecutar inyecciones SQL.*

```
111      /* access modifiers changed from: private */
112      public void deshabilitatBotones() {
113          this.botonEscanear.setEnabled(false);
114          this.botonSiguiente.setEnabled(false);
115      }
116
117      /* access modifiers changed from: private */
118      public void habilitarBonotes() {
119          this.botonEscanear.setEnabled(true);
120          this.botonSiguiente.setEnabled(true);
121      }
```

*Análisis: Varios usuarios reportaron funciones rotas. Probablemente se deba a la enorme cantidad de errores de tipeo (typos) en el código (En este caso “habilitarBonotes” en lugar de “habilitarBotones”; y “deshabilitatBotones” en lugar de “deshabilitarBotones”). Se ejecutaron pruebas de desensamblado con distintas utilidades para garantizar que esto no fuera un error de decompilación.*

```
public static final int clear_text_end_icon_content_description = 2131820602;
public static final int codigo_area_mas_numeor = 2131820603;
public static final int codigo_postal = 2131820604;
public static final int common_google_play_services_enable_button = 2131820605;
public static final int common_google_play_services_enable_text = 2131820606;
public static final int common_google_play_services_enable_title = 2131820607;
```

*Análisis: Nuevamente, typo. “numeor” en lugar de “numero”.*

```
public static final int horas_10 = 2131820671;
public static final int horas_48 = 2131820672;
public static final int horas_restantes = 2131820673;
public static final int hubo_error = 2131820674;
public static final int hubo_error_desc = 2131820675;
public static final int icon_content_description = 2131820676;
public static final int landing_pie_subtitulo = 2131820677;
public static final int landing_subtitulo = 2131820678;
public static final int landing_titulo = 2131820679;
public static final int localidad_departamento_partido = 2131820680;
public static final int localidades = 2131820681;
public static final int login_pregunta_datos_personales = 2131820682;
public static final int mas_informacion = 2131820683;
public static final int mas_informacion_subrayado = 2131820684;
public static final int masculino = 2131820685;
public static final int mensaje_error_escanear_dni = 2131820686;
public static final int ministerio_de_salud = 2131820687;
public static final int mira_recomendaciones_de_salud = 2131820688;
public static final int msg_evitar_salir = 2131820689;
```

*Análisis: Typo. "masculio" en lugar de "masculino".*



```

2685 public static final int path_password_eye = 2131820757;
2686 public static final int path_password_eye_mask_strike_through = 2131820758;
2687 public static final int path_password_eye_mask_visible = 2131820759;
2688 public static final int path_password_strike_through = 2131820760;
2689 public static final int permiso_circular = 2131820761;
2690 public static final int permitir = 2131820762;
2691 public static final int piso = 2131820763;
2692 public static final int podes_circular = 2131820764;
2693 public static final int prefijo_telefono = 2131820765;
2694 public static final int pregunta_actualizar_certificado = 2131820766;
2695 public static final int pregunta_desvincular_dni = 2131820767;
2696 public static final int provincia = 2131820768;
2697 public static final int provinvia_y_telefondo = 2131820769;
2698 public static final int puerta = 2131820770;
2699 public static final int quedate_en_casa = 2131820771;
2700 public static final int quedate_en_casa_azul = 2131820772;
2701 public static final int realiza_autodiagnostico = 2131820773;
2702 public static final int recomendacion_test_cada_x_horas = 2131820774;
2703 public static final int search_menu_title = 2131820775;
2704 public static final int seleccionar_sintoma = 2131820776;
2705 public static final int sexo = 2131820777;
2706 public static final int si = 2131820778;
2707 public static final int siguiente = 2131820779;
2708 public static final int sin_conexion_intenet = 2131820780;
2709 public static final int sintoma_dos_label = 2131820781;
2710 public static final int sintoma_perdida_gusto = 2131820782;
2711 public static final int sintoma_perdida_olfato = 2131820783;
2712 public static final int sintoma_uno_label = 2131820784;
2713 public static final int sintomas_titulo = 2131820785;
2714 public static final int status_bar_notification_info_overflow = 2131820786;
2715 public static final int temperatura_error_limite = 2131820787;
2716 public static final int temperatura_vacia_error = 2131820788;
2717 public static final int terminos = 2131820789;
2718 public static final int terminos_condiciones = 2131820790;
2719 public static final int texto_resultado_negativo = 2131820791;
2720 public static final int texto_resultado_positivo_dos = 2131820792;
2721 public static final int texto_resultado_positivo_uno = 2131820793;
2722 public static final int texto_terminos = 2131820794;
2723 public static final int titulo_en_evaluacion = 2131820795;
2724 public static final int token_de_seguridad = 2131820796;
2725 public static final int token_de_seguridad_usuario_con_qr = 2131820797;
2726 public static final int tu_direccion = 2131820798;
2727 public static final int tu_informacion_esta_protegida = 2131820799;
2728 public static final int tus_datos_de_contacto = 2131820800;
2729 public static final int txt_rocomedar_tiempo_autodiagnostico = 2131820801;
2730 public static final int txt_sin_sintomas_title = 2131820802;

```

*Análisis: Typo. “provinvia” en lugar de “provincia”.*

```

37 public UsuarioRemoto confirmarAutodiagnostico(String str, String str2, AutoevaluacionRemoto autoevaluacionRemoto) {
38     try {
39         return (UsuarioRemoto) this.covidRetrofit.obtenerAutoEvaluacionService().confirmarAutoevaluacion(str, str2, autoevaluacionRemoto).execute().body();
40     } catch (IOException unused) {
41         return null;
42     }
43 }

```

*Análisis: La función de autoevaluación (la cual muchos usuarios indicaron no funcionaba), es llamada como autoevaluacoín (sic), lo cual explicaría el comportamiento errático.*

*Análisis: El token del sistema de monitoreo New Relic es divulgado en el código. Si bien es un token de sólo escritura, podría permitir un ataque de tipo stuffing o billing attack.*

*Análisis: Ciertas respuestas JSON se escriben sin sanitizar, de forma precaria en lugar de usar una librería específica.*

```
sources\c\clad\dc.java sources\c\clad\d.java X
```

```
sources\c\clad\d.java > {} c.c.a.d  
1 package c.c.a.d;  
2   
3 /* compiled from: PermisoDeUbicacion */  
4 public enum d {  
5     SIN_PERMISO,  
6     TODO_EL_TIEMPO,  
7     SOLO_CON_LA_APLICACION_VISIBLE,  
8     NUNCA  
9 }  
10
```

**Análisis:** La función de seguimiento tiene programada la configuración "TODO EL TIEMPO".

```
291
292     public static Drawable c(Drawable drawable) {
293         return (VERSION.SDK_INT < 23 && !(drawable instanceof b.h.g.j.a)) ? new b.h.g.j.d(drawable) : drawable;
294     }
295
296     public static d d(Context context) {
297         if (VERSION.SDK_INT >= 29) {
298             return e(context);
299         }
300         return b.h.f.a.a(context, "android.permission.ACCESS_FINE_LOCATION") == 0 ? d.TODO_EL_TIEMPO : d.SIN_PERMISO;
301     }

```

*Análisis: En varias instancias, se evalúa en absolutos: si la aplicación tiene el permiso absoluto, o ninguno.*

```

2597     public static d a(b.b.k.i iVar, int i2) {
2598         d dVar;
2599         String str = "android.permission.ACCESS_FINE_LOCATION";
2600         boolean a2 = b.h.e.a.a((Activity) iVar, str);
2601         if (VERSION.SDK_INT >= 29) {
2602             boolean a3 = b.h.e.a.a((Activity) iVar, "android.permission.ACCESS_BACKGROUND_LOCATION");
2603             if (!a2 || !a3) {
2604                 return e(iVar);
2605             }
2606             return d.NUNCA;
2607         } else if (a2) {
2608             return d.NUNCA;
2609         } else {
2610             if (b.h.f.a.a((Context) iVar, str) == 0) {
2611                 dVar = d.TODO_EL_TIEMPO;
2612             } else {
2613                 dVar = d.SIN_PERMISO;
2614             }
2615             return dVar;
2616         }
2617     }
2618 }

```

*Análisis: Otra de las instancias donde se evalúa en absolutos.*

```

1 package c.c.a.d;
2
3 import c.c.a.e.b;
4 import com.globant.pasaportesanitario.locationtracker.ReceiverArranqueDeDispositivo;
5
6 /* compiled from: ReceiverArranqueDeDispositivo */
7 public class h implements b {
8     public h(ReceiverArranqueDeDispositivo receiverArranqueDeDispositivo) {
9     }
10
11     public void mostrarDialogoDeActualizarForzado() {
12     }
13 }
14

```

**Análisis:** La aplicación intenta detectar el arranque del dispositivo.



```

sources\cicla\dh.java x
sources\cicla\dh.java > {} c.c.a.d
1 package c.c.a.d;
2
3 import c.c.a.e.b;
4 import com.globant.pasaportesanitario.locationtracker.ReceiverArranqueDeDispositivo;
5
6 /* compiled from: ReceiverArranqueDeDispositivo */
7 public class h implements b {
8     public h(ReceiverArranqueDeDispositivo receiverArranqueDeDispositivo) {
9     }
10
11     public void mostrarDialogoDeActualizarForzado() {
12     }
13 }
14

```

*Análisis: Una vez detectado el arranque, la aplicación obliga al usuario a instalar las últimas actualizaciones para poder operar.*

```

sources\cicla\dh.java x
sources\cicla\dh.java > {} c.c.a.d
1 package c.c.a.d;
2
3 import android.util.Log;
4 import c.a.a.a.a;
5 import e.a.m.b;
6
7 /* compiled from: RepositorioRastreoLocalizacion */
8 public class o implements b<Throwable> {
9     public o(q qVar) {
10     }
11
12     public void accept(Object obj) throws Exception {
13         Throwable th = (Throwable) obj;
14         String name = o.class.getName();
15         StringBuilder a2 = a.a("Error al enviar la ubicacion: ");
16         a2.append(th.getMessage());
17         Log.e(name, a2.toString());
18     }
19 }
20

```

*Análisis: La aplicación guarda registros de cada vez que fue imposible enviar la ubicación del usuario al servidor central, para reintentar más tarde.*

```

37
38  /* access modifiers changed from: private */
39  public void crearDialogo() {
40      b bVar = new b(requireContext(), R.style.AlertDialogTheme);
41      AlertController.b bVar2 = bVar.f521a;
42      bVar2.f85f = bVar2.f80a.getText(R.string.autodiagnostico_confirmacion);
43      AlertController.b bVar3 = bVar.f521a;
44      bVar3.f87h = bVar3.f80a.getText(R.string.autodiagnostico_confirmacion_message);
45      AnonymousClass3 r1 = new OnClickListener() {
46          public void onClick(DialogInterface dialogInterface, int i) {
47              if (a.c(AutodiagnosticoAntecedentesFragment.this.getContext())) {
48                  AutodiagnosticoAntecedentesFragment.this.viewModel.enviarResultadosAutoevaluacion();
49              } else {
50                  AutodiagnosticoAntecedentesFragment.this.crearDialogoInternet();
51              }
52          }
53      };

```

*Análisis: Las autoevaluaciones son enviadas a un servidor, cuando podrían ser totalmente basadas en el lado cliente.*

```

21  public Object call() throws Exception {
22      UsuarioBD usuario = this.f3104c.f3106b.getUsuario();
23      this.f3104c.f3105a.enviarUbicacion(usuario.dni.toString(), usuario.sexo, Double.toString(this.f3103b.getLatitude()), Double.toString(this.f3103b.getLongitude()), Double.toString(this.f3103b.getAltitude()));
24      return Boolean.valueOf(true);
25  }

```

*Análisis: Envío de ubicación con datos del usuario.*

```

126  private void iniciarRastreoDeUsuario(int i, String[] strArr, int[] iArr) {
127      int i2 = VERSION.SDK_INT;
128      if (i2 >= 29) {
129          d a2 = a.a(strArr, iArr);
130          if (a2 == d.TODO_EL_TIEMPO || a2 == d.SOLO_CON_LA_APLICACION_VISIBLE) {
131              this.viewModel.lanzarServicoDeRastreo();
132          }
133      } else if (i2 >= 23) {
134          boolean z = false;
135          if (iArr.length > 0 && iArr[0] == 0) {
136              z = true;
137          }
138          if (z) {
139              this.viewModel.lanzarServicoDeRastreo();
140          }
141      }
142  }

```

*Análisis: No importa las decisiones del usuario, son artificiales. La app siempre lanzará servicios de rastreo.*

Herramientas de firmas líderes del mercado han encontrado resultados interesantes:

There is 'https://expo.io:443/@sergio[REDACTED]/COVID19-Ministerio-de-Salud' found in file 'host/exp/exponent/MainActivity.java':

```
line 31:         return "https://expo.io:443/@sergio[REDACTED]/COVID19-Ministerio-de-Salud";
```

There is 'https://expo.io:443/@sergio[REDACTED]/COVID19-Ministerio-de-Salud' found in file 'host/exp/exponent/generated/AppConstants.java':

```
line 14:     public static String INITIAL_URL =  
"https://expo.io:443/@sergio[REDACTED]/COVID19-Ministerio-de-Salud";
```

```
line 22:         arrayList.add(new a("https://expo.io:443/@sergio[REDACTED]/COVID19-Ministerio-de-Salud", "assets://shell-app-manifest.json", "application/json"));
```

*ImmuniWeb: Análisis de código de una versión anterior de la aplicación demuestra una filtración del nombre del autor.*

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

sergio[REDACTED]@gmail.com

pwned?

Oh no — pwned!

Pwned on 3 [breached sites](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

*HaveIBeenPwnd: Análisis de la dirección de email del autor demuestra que ha sido vulnerado en varias oportunidades.*

## Risk Score



61

## Risky Behaviors

Connects to the Internet

Encrypt or Decrypt data

Exist unused permissions

Gets geographic location

Gets the alphabetic name of current registered operator

Gets the numeric name (MCC+MNC) of current registered operator

Gets the unique device ID, IMEI for GSM and MEID for ESN or ESN for CDMA phones

Loads and links the dynamic library

Open camera

Utilizes Java reflection

*SandDroid: La aplicación utiliza permisos abusivos. Obtuvo un puntaje de 61/100 en riesgo.*

**Potentially** Backup mode enabled

### Description

Android performs by default a full backup of applications including the private files stored on /data partition. The Backup Manager service uploads those data to the user's Google Drive account.

*OstorLab: La aplicación solicita datos de salud al usuario, mientras tiene la función de resguardo en la nube de Google Drive activada. Esto supone un riesgo ante la posible difusión de datos de la más alta confidencialidad.*



write	/data/data/ar.gob.coronavirus/shared_pre fs/com.newrelic.android.agent.v1_ar.gob. coronavirus.xml	PD94bWwgdmVyc2l2bWJ0nMS4wJyBlbmNvZGluzZ0ndXRmLTgnIHNOYW5kYWxvbmU9J3llcygcPz24KPG1hcD4KICAgIDxz dHJpbmcgbmFtZT0iZGV2aWVuNWQXJjaGloZWNOdXJlIj5hcml2N2w8L3N0cmLuZz4KICAgIDxz dHJpbmcgbmFtZT0iZGV2aWVuNWQXQipjdjNmY5NDBkLWJmNTItNGlxNy04M2lwLWE1MzdiYTE0NTdmNTwvc3RyaW5nPgogICAgPHN0cmLuZyBuYWY1IPSJhcHBCdWlsZCI+MTE1PC9zdHJpbmc+CiAgICA8aW50IG5hbWU9InZlcnNpb25Db2RlIiB2YWx1ZT0iMTE1liAvPgogICAgPHN0cmLuZyBuYWY1IPSJhZ2VudFZlcnNpb24iPjUuMjUuMTwvc3RyaW5nPgogICAgPHN0cmLuZyBuYWY1IPSJkZXZpY2Vs dU5aUaW1lj4yLjEuMDwvc3RyaW5nPgogICAgPHN0cmLuZyBuYWY1IPSJkZXZpY2Vnbn2RlbiCI+SDYwMTE8L3N0cmLuZz4KICAgIDxz dHJpbmcgbmFtZT0iYWdlbnROYWY1Ij5BbmRyb2lkQWdlbnQ8L3N0cmLuZz4KICAgIDxz dHJpbmcgbmFtZT0iZGV2aWVuNTlTWfudWZhY3R1cmVylj51bmtub3duPC9zdHJpbmc+CiAgICA8c3RyaW5nIG5hbWU9ImFwcE5hbWUiPkNvdmlkMTktQVl8L3N0cmLuZz4KICAgIDxz dHJpbmcgbmFtZT0icGFja2FnZUlklj5hc5nb2luY29yb25hdml ydXM8L3N0cmLuZz4KPC9tYXA+Cg==
-------	---	---

*SandDroid: La aplicación escribe varios archivos XML con contenido codificado en Base64.*

```
fish /home/plaguedoktor/Projects/COVID-1984
```

Archivo Editar Ver Buscar Terminal Ayuda

```
== " | base64 -d
```

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
```

```
<map>
```

```
  <string name="deviceArchitecture">armv7l</string>
```

```
  <string name="deviceId">7c6f940d-bf52-4b17-83b0-a537ba1457f5</string>
```

```
  <string name="appVersion">3.0.7</string>
```

```
  <string name="appBuild">115</string>
```

```
  <int name="versionCode" value="115" />
```

```
  <string name="agentVersion">5.25.1</string>
```

```
  <string name="deviceRunTime">2.1.0</string>
```

```
  <string name="deviceModel">H6011</string>
```

```
  <string name="agentName">AndroidAgent</string>
```

```
  <string name="deviceManufacturer">unknown</string>
```



```
  <string name="appName">Covid19-AR</string>
```

```
  <string name="packageId">ar.gob.coronavirus</string>
```

```
</map>
```

✓ COVID-1984

*Análisis: Decodificando el contenido del archivo XML encontramos que la aplicación está guardando datos específicos sobre el dispositivo en el que corre, como ID de Dispositivo, Modelo y Marca. En este caso, el dispositivo es virtual (falso) por lo que ninguna información relevante fue filtrada.*

Country	Url	IP
 China	N/A	203.208.39.239
N/A	http://localhost/	N/A
 Taiwan	https://play.google.com/store/apps/details?id=	172.217.27.142
 United States	https://www.argentina.gob.ar/solicitar-certificado-unico-habilitante-para-circulacion-emergencia-covid-19	104.27.182.13
 United States	https://plus.google.com/	31.13.77.55
 United States	https://api.app.covid.ar/	75.2.14.245
 United States	N/A	151.101.130.110
 United States	N/A	151.101.66.110
 United States	N/A	151.101.2.110
 United States	N/A	151.101.194.110

*SandDroid: Todas las interacciones de la aplicación son con servidores en el extranjero. Esto supone un grave riesgo a la privacidad de la información médica privada del usuario.*

Hostname	IP:Port	SSL Encryption	Websec Server Security	Domain Domain Security
mobile-collector.newrelic.com:443	151.101.66.110:443	F	B	No risks found
www.youtube.com:443	172.217.13.174:443	A-	A	1543 malicious websites found
www.argentina.gob.ar:443	104.27.182.13:443	A+	A	375 malicious websites found
api.app.covid.ar:443	75.2.14.245:443	A-	C	No risks found

*Immuniweb: Toda la información de la aplicación (críticamente sensible al ser información de salud) son enviados a un servidor en Amazon Estados Unidos, con calificación de seguridad "C" (Mala).*

## Summary of api.app.covid.ar Website Security Test

### FINAL GRADE



### DNS

#### SERVER IP

75.2.14.245

#### REVERSE DNS

a8852a2a614eba584.awsglobalacce...

### INFO

#### DATE OF TEST

May 12th 2020, 03:37

#### SERVER LOCATION

Tracy 

*Immuniweb: Detalles de la calificación del servidor.*

## HTTP Headers Security Analysis

Some HTTP headers related to security and privacy are missing or misconfigured.

Misconfiguration or weakness

### MISSING REQUIRED HTTP HEADERS

Strict-Transport-Security

X-Frame-Options

X-XSS-Protection

X-Content-Type-Options

Expect-CT

Feature-Policy

## Content Security Policy Analysis

### CONTENT-SECURITY-POLICY

The header was not sent by the server.

Misconfiguration or weakness

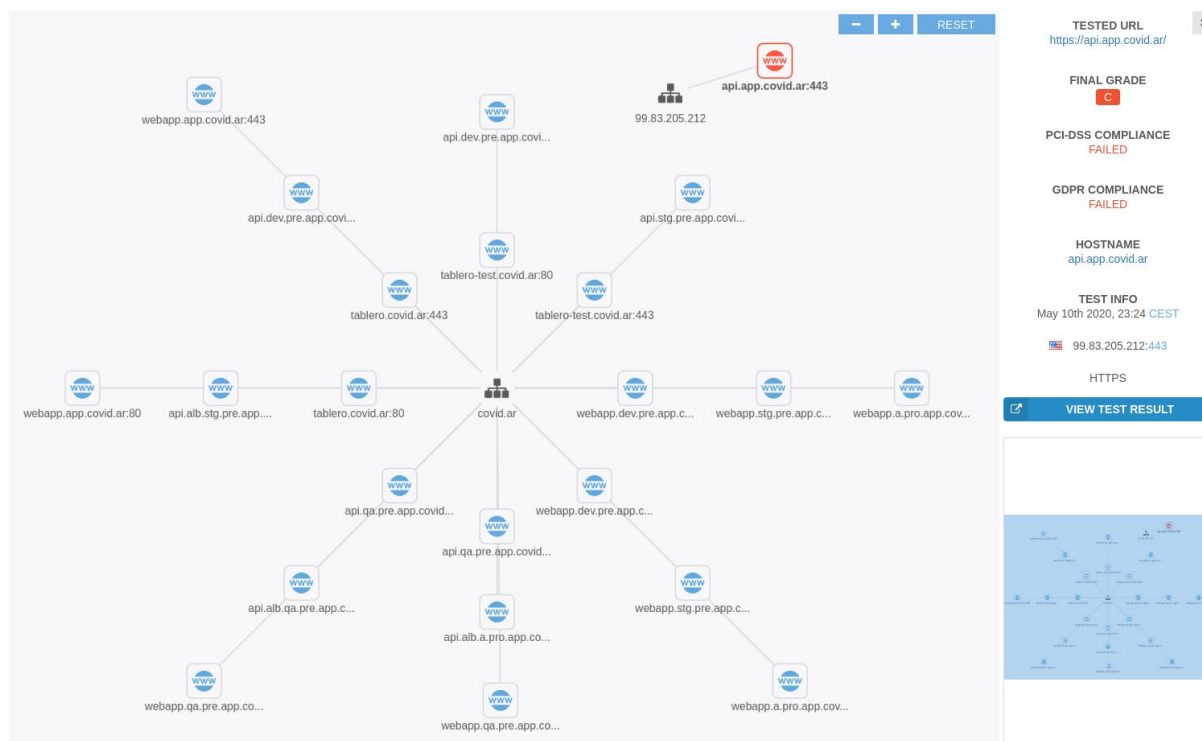
*Immuniweb: Ciertos encabezados de seguridad no están configurados en la API, esto podría indicar que no hay un Firewall de Aplicación instalado, o que no está correctamente configurado.*

### REQUIREMENT 6.6

No WAF was detected on the website. Implement a WAF to protect the website against common web attacks.

Misconfiguration or weakness

*Immuniweb: Tal como suponía el caso anterior, no se ha detectado un WAF (Firewall de Aplicación) emplazado.*



*Immuniweb: Mapa de reconocimiento de subdominios de la aplicación. Todos heredan la misma calificación de seguridad: C.*

Otras vulnerabilidades son ampliadas y explicadas en profundidad en la charla que representa a este Whitepaper. Es coherente entonces afirmar que **es fundada la preocupación por el tratamiento de los datos de usuario, y la posible vulneración de su privacidad mediante el uso de esta aplicación.**

## ACERCA DE VENATOR

Venator es una aplicación escrita en LUA, para sistemas Unix. Utiliza la API de Twitter para obtener información pública y generar piezas de inteligencia de fuentes abiertas (OSINT) para investigar acciones de propaganda política en dicha red social.

Todo su comportamiento es legal y cumple con los términos y condiciones de la plataforma.

Entre sus funciones se destacan la capacidad de analizar un perfil en busca de rasgos o comportamientos que indiquen una posible actividad propagandística o automatizada; analizar hashtags utilizados por un usuario específico, cuantificándolos como una nube de palabras; analizar interacciones de un usuario con otras cuentas, cuantificándolas; analizar tendencias específicas para obtener en tiempo real un informe sobre sus participantes y los mensajes donde las incluyen; entre otros.

Fue escrita por el autor del presente trabajo, y será liberada bajo licencia BSD.

## HERRAMIENTAS UTILIZADAS

- Obtención de datos y procesamiento: Venator.lua (<https://github.com/MauroEldritch/COVID-1984>), Twitter API, Twitter LUA Library, Twitter Ruby Gem, Lua, Ruby.
- Decompiladores: JADX, APKTool, Decompile Android (<http://www.decompileandroid.com/>).
- Análisis de Código: VCG (<https://github.com/nccgroup/VCG>), CodeWarrior (<https://github.com/CoolerVoid/codewarrior>), Immuniweb (<https://www.immuniweb.com/mobile/>), OstorLabs (<https://www.ostorlab.co/scan/mobile/>), SandDroid (<http://sanddroid.xjtu.edu.cn/#upload>), Drozer (<https://labs.f-secure.com/tools/drozer/>).

## LECTURA COMPLEMENTARIA

### MEDIOS

[1] Internet of Business: Propaganda Chatbots and Social Media Manipulation -

<https://internetofbusiness.com/propaganda-bots-social-media-manipulation/>

[2] Washington Post: - Twitter is sweeping out fake accounts like never before -

<https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/>

[3] Alexander Nix (Cambridge Analytica CEO) admits a contract with Argentina -

<https://www.youtube.com/watch?v=K609-CQtO6s>

[4] Periodismo para Todos, Canal 13 Argentina: Conoce a los Ciber-K -

[https://www.eltrecetv.com.ar/videos/periodismo-para-todos-2012/conoce-a-los-ciber-k\\_022860](https://www.eltrecetv.com.ar/videos/periodismo-para-todos-2012/conoce-a-los-ciber-k_022860)

[5] Scientific America: How Twitter Bots Help Fuel Political Feuds -

<https://www.scientificamerican.com/article/how-twitter-bots-help-fuel-political-feuds/>

[6] BoxCryptor: Social Bots, Detection and Impact on Social and Political Events -

<https://www.boxcryptor.com/en/blog/post/social-bots-detection-examples-of-political-impact/>

[7] La Nación: Chaco: Dos legisladores proponen responsabilizar a los medios digitales... -

<https://www.lanacion.com.ar/sociedad/chaco-dos-legisladores-proponen-responsabilizar-a-los-medios-digitales-de-comunicacion-por-los-comentarios-de-sus-foristas-nid1684544>

[8] La Nación: Un Senador del Frente de Todos propone la regulación de las redes sociales -

<https://www.lanacion.com.ar/politica/un-senador-del-frente-todos-propone-regulacion-nid2356872>

[9] Twitter: Senador Luenzo -

<https://twitter.com/SenadorLuenzo/status/1251564120408821760>

[10] Infobae: Los Detalles del protocolo de ciberpatrullaje -

<https://www.infobae.com/politica/2020/04/19/los-detalles-del-protocolo-de-ciberpatrullaje-que-impulsa-el-gobierno-que-busca-regular-y-cuales-son-los-puntos-mas-cuestionados/>

[11] Red de Defensa de los Derechos Digitales: Detenido por Tuitear -

<https://r3d.mx/2020/04/21/detenido-por-tuitear-el-ciberpatrullaje-contra-los-derechos-humanos-en-argentina/>

[12] Roberts, Carlos Raymundo. Aguanten los K: Una mirada mordaz sobre la increíble Argentina de estos tiempos. Sudamericana. ISBN: 9789500740593 -

<https://books.google.com.uy/books?id=HAVIFN1Rf4kC&lpg=PT70&ots=tZgmwKBpSC&dq=cyber%20k%20la%20nacion&pg=PT1#v=onepage&q=cyber%20k%20la%20nacion&f=false>

[13] Diario Perfil: Trolls y fondos públicos: Así se gesta el relato 2.0 en la era Cambiemos -

<https://www.perfil.com/noticias/politica/trolls-y-fondos-publicos-asi-se-gesta-el-relato-20-en-la-era-cambiemus.phtml>

[14] Noticias: Quién es el profesor de los Cyber K -

<https://noticias.perfil.com/noticias/politica/quien-es-el-profesor-de-los-trolls-k.phtml>

[15] Tribuna: Cómo actúan los trolls K y quién los organiza -

<https://periodicotribuna.com.ar/24208-exclusivo-como-actuan-los-trolls-k-y-quien-los-organiza.html>

[16] Infobae: - El insólito manual de micro militancia K para resistir al gobierno -

<https://www.infobae.com/2016/01/14/1782988-el-insolito-manual-micro-militancia-k-resistir-al-gobierno/>

[17] Infobae: Un debate sobre los Bots en Campaña -

<https://www.infobae.com/tecnologia/2019/08/09/satisface-a-mauricio-caricia-significativa-y-otras-razones-insolitas-viralizadas-en-twitter-abrieron-un-debate-sobre-los-bots-en-campana/>

[18] El Observador (Uruguay): Simpsons sin censura -

<https://www.elobservador.com.uy/nota/simpsons-sin-censura-20114111920>

[19] A24: El día que Cristina Kirchner censuró en un canal de televisión a Alberto Fernández -

[https://www.a24.com/farandula/dia-cristina-kirchner-censuro-canal-television-alberto-fernandez-05202019\\_S1YXIRI64](https://www.a24.com/farandula/dia-cristina-kirchner-censuro-canal-television-alberto-fernandez-05202019_S1YXIRI64)

[20] RT: Facepopular, un paraíso de red social que integra a Latinoamérica -

<https://actualidad.rt.com/actualidad/view/110238-facepopular-redes-facebook-latinoamerica>



[21] Infobae: El Facepopular no llega al millón de usuarios militantes - <https://www.infobae.com/2014/09/15/1594967-el-facepopular-no-llega-al-millon-usuarios-militantes/>

[22] La Nación: El Señor de los trolls - <https://www.lanacion.com.ar/politica/el-senor-de-los-trolls-asi-functiona-el-mundo-de-las-campanas-sucias-y-las-bases-de-datos-irregulares-nid2286145>

[23] WayBack Machine: FacePopular.net - <https://web.archive.org/web/20130710212226/http://www.facepopular.net/>

[24] La Nación: Cómo funciona la app CuidAR, de uso obligatorio para quienes vuelven al trabajo durante la cuarentena - <https://www.lanacion.com.ar/tecnologia/app-cuidar-permiso-coronavirus-covid19-nid2363457>

[25] La Política Online: Manual de Micromilitancia K (PDF) - [https://www.lapoliticaonline.com/files/content/95/95301/TECNICAS\\_DE\\_RESISTENCIA\\_AC\\_TIVA\\_2.pdf](https://www.lapoliticaonline.com/files/content/95/95301/TECNICAS_DE_RESISTENCIA_AC_TIVA_2.pdf)

[26] Infobae: La SUBE quedará habilitada sólo para trabajadores esenciales y exceptuados - <https://www.infobae.com/sociedad/2020/05/16/la-sube-quedara-habilitada-solo-para-trabajadores-esenciales-y-exceptuados/>

[27] Trends IN - <https://trends24.in/argentina/>

## TÉCNICAS

[A] IEEE: How Political Campaigns Weaponize Social Media Bots - <https://spectrum.ieee.org/computing/software/how-political-campaigns-weaponize-social-media-bots>

[B] BRADSHAW, Samantha; HOWARD, Philip N: Challengin Truth and Trust: A Global Inventory of Organized Social Media Manipulation - <http://comprop.oii.ox.ac.uk/research/cybertroops2018/> & <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf> & [http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct\\_appendix.pdf](http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct_appendix.pdf)

[C] Google Inc. - Transparency Report, Government Requests [https://transparencyreport.google.com/user-data/overview?user\\_requests\\_report\\_period=series:requests.accounts;authority:AR;time:&lu=legal\\_process\\_breakdown&legal\\_process\\_breakdown=expanded:0](https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests.accounts;authority:AR;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded:0)

[D] Indiana University, Botometer - <https://botometer.iuni.iu.edu/#/>

[E] RubyGems: Twitter - <https://rubygems.org/gems/twitter/>