POLÍTICA

Cuáles son las principales hipótesis detrás del hackeo a la base del Renaper

Un pirata informático aseguró tener los datos identificatorios de 45 millones de argentinos, aunque el organismo negó que hubiera habido una descarga masiva. La secuencia de la filtración que evidenciaría la vulnerabilidad del sistema

Por **Mariel Fitz Patrick**, **Iván Ruiz** y

La noticia se conoció a principios de mes. Un hacker publicó a través de la cuenta de twitter @AnibalLeaks los **datos privados de 44 figuras públicas argentinas con su foto original del DNI**. La difusión encendió alarmas en el Gobierno. Eran datos sensibles que incluían los números de documentos y, en el caso del Ministro de Seguridad, Aníbal Fernández, hasta su

comenzaron a hacerse de forma virtual y ese número pasó a funcionar como el código de seguridad de las tarjetas de crédito.

Las preguntas que despertaron preocupación se centraron básicamente en dos: **¿Tendrá el hacker datos de los 45 millones de argentinos? ¿Es la base de datos del Renaper suficientemente segura?** Expertos consultados por **Infobae** sostienen que -como el propio hacker afirma- **es factible que se haya robado los datos de identificación de todos los argentinos**. Hay varios indicios. Como ejemplo del material en su poder, el pirata informático expuso **una muestra de la base de datos cuyos números de DNI son correlativos**. No es todo: dos personas le pidieron datos particulares al azar o los propios, y el hacker les respondió con la información solicitada, con foto incluida.

Sin embargo, fuentes oficiales a las que contactó este medio sostienen, en cambio, la hipótesis cker habría ingresado en distintas oportunidades -afirman- y habría extraído pequeñas porciones de datos.

Los especialistas en tecnología que estuvieron siguiendo las novedades de la filtración, coincidieron en señalar la vulnerabilidad de la base de datos del Renaper. Entre sus falencias, remarcaron que el organismo no cuenta con un sistema de alertas que impida la consulta masiva de datos en un determinado período de tiempo.

La cuenta de @AnibalLeaks que usó el hacker y luego fue suspendida por Twitter

A la base del Renaper tienen acceso decenas de organismos públicos y empresas privadas que realizan consultas permanentemente para validar datos para distintas operaciones informáticas, que incluyen desde trámites hasta compras con tarjeta de crédito. Cuando se desató la pandemia, **el Ministerio de Salud de la Nación se convirtió en uno de los principales usuarios de esa base de datos**. Y aplicaciones lanzadas por el gobierno como CuidAR, requerida para tramitar el certificado de circulación en la cuarentena, toman los datos del Renaper

El organismo habilitó una docena de datos de cada argentino para que la cartera sanitaria pueda consultarlos en la base a través de credenciales informáticas. Salud, a su vez, extendió ese permiso a cientos de actores internos de todo el país, que cargan los resultados de los test de COVID-19 y vacunación en el sistema integrado de salud SISA.

“Inicialmente el Renaper dijo que la filtración fue posible mediante credenciales que están asignadas al Ministerio de Salud. Incluso se habló de ocho personas que tenían estas credenciales. Pero más allá de lo cuestionable de que el Renaper esté mostrando nuestros datos a otros organismos públicos, **lo que quedó en evidencia es que no tiene un sistema de control que limite la cantidad de requerimientos en determinada cantidad de minutos, horas o por día.** La excusa del Renaper fue que Salud tenía canilla libre por la carga de datos en el

programador y consultor informático **Javier Smaldone**, uno de los que sufrió la filtración de sus datos en Twitter por parte del hacker.

El consultor informático Javier Smaldone fue uno de los que vio su foto expuesta en Twitter por el hacker

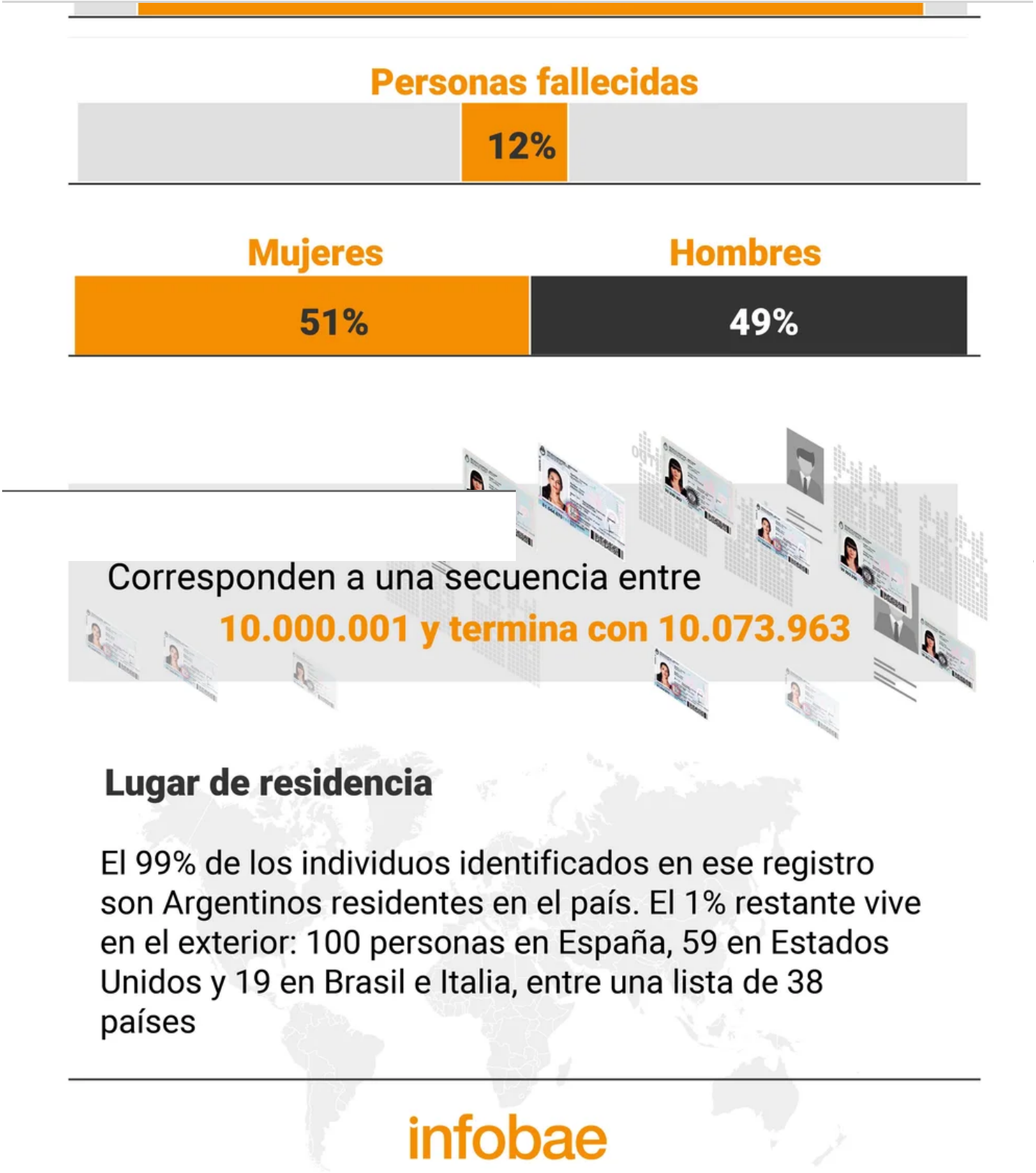
"Julito" López se explayó sobre cómo puede haber ocurrido el hackeo: "La interconexión entre el Ministerio de Salud y el Renaper tiene un usuario y un password, y un Token de seguridad quizás. Alguien robó ese usuario y password que usan los servidores para hablarse entre ellos, no lo usa una persona, sino las máquinas que se conectan entre sí. Lo que robaron es el usuario

Las fuentes gubernamentales consultadas por **Infobae** precisaron que la cantidad de consultas diarias que utilizan las credenciales informáticas del Ministerio de Salud oscilan entre 600.000 y 800.000 por día. Y que **en los días previos a que se hiciera público el robo de datos, no detectaron un aumento significativo en la cantidad de consultas.**

"Está previsto que haya cortes del acceso inmediato por cuotas de datos requeridos y por concurrencia, es decir, cuando se intenta ingresar insistentemente. Pero en ninguno de los casos fueron detectados en este robo de datos", explicaron esas fuentes oficiales en *off the record.*

Una muestra de los datos robados

uestra de 60.000 registros de la base de datos robada del Renaper, y luego filtrada por el hacker. De su análisis se desprende que **los DNI tienen una secuencia correlativa. Es decir, van de los 10.000.001 a los 10.073.963 con sus respectivos números de trámite.** Esto tiene un correlato con la edad: el 88% de la muestra total tiene 70 años de edad. La más longeva es una mujer de 107 años nacida en 1914 en la provincia de Salta, y reportada en el registro sin aviso de fallecimiento.El resto son personas mayores de 53 años. Solo el 12 % de las 60.000 corresponde a personas fallecidas El 51% son mujeres y el 49% son hombres.



El 16 % del total de DNIs de la muestra corresponde a la provincia de Santa Fe; el 15% a Córdoba, el 10% a Buenos Aires y el resto en otras provincias. Solo el 2% (1.216 personas) de esos 60.000 son individuos que viven en la Ciudad de Buenos Aires.

Los especialistas consultados por este medio coinciden en que **la correlación numérica de los números de DNI de la muestra filtrada indicaría que el hacker pudo acceder a grandes lotes**

“Filtró la base de 60.000 registros correlativos para darle veracidad a su anuncio de que accedió a los DNI de los 45 millones de argentinos. Y no es menor que **las fotos filtradas estaban en su formato original, en alta definición, como las tiene el Renaper**. En mi caso, por ejemplo, era mi foto real del DNI, sin el parche que suelo usar en el ojo”, explicó **Julio López**, especialista en tecnología a este medio. López fue uno de los primeros al que el pirata informático arrobó en Twitter para avisarle del hackeo, y como el experto lo ignoró, publicó su foto del DNI.

El hacker publicó la foto original del DNI del especialista en tecnología Julio López, con la leyenda en inglés "Linda imagen"

una descarga masiva de la totalidad de los documentos de la población argentina, accediendo al usuario y contraseña de la interfaz por la que se conecta algún organismo público con la base de datos del Renaper", agregó López.

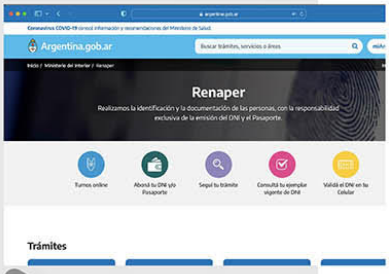
La secuencia de las filtraciones

Smaldone advirtió que la secuencia de cómo ocurrieron las distintas filtraciones por parte del hacker reafirma la hipótesis de que es siempre el mismo y que, **o robó la base con los datos de los 45 millones de argentinos, o sigue teniendo acceso a los registros.**

3

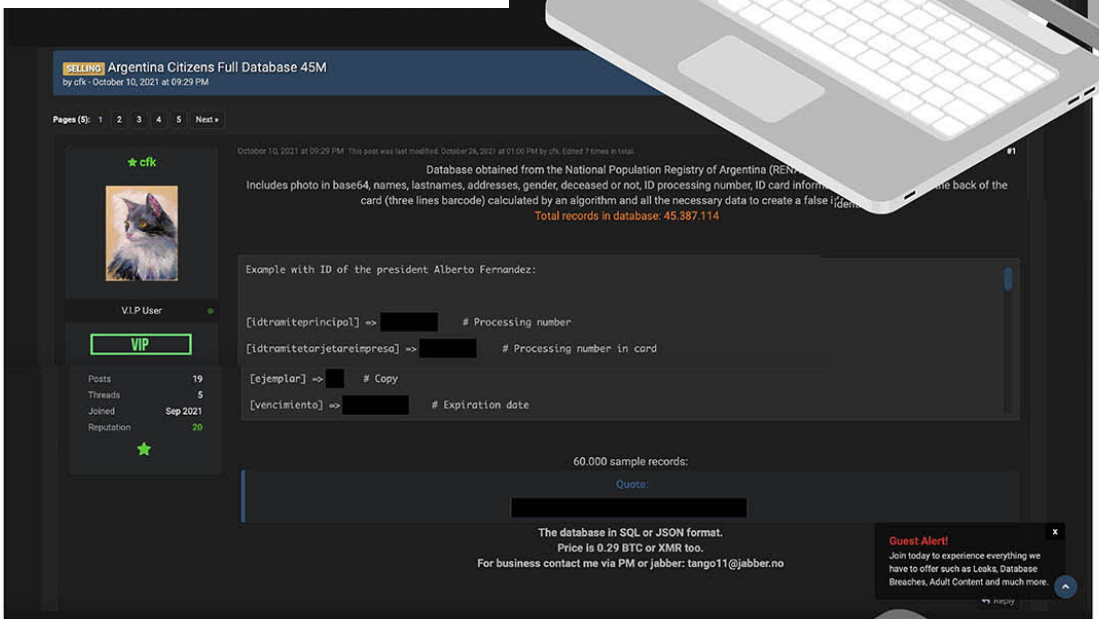
El RENAPER da de baja a credenciales de acceso del Ministerio de Salud

Identificadas como sospechosas de haber sido usadas para la filtración de los datos



4

En un foro de piratería el hacker **ofreció a la venta el acceso a los datos personales** y publicó un correo electrónico de contacto



5

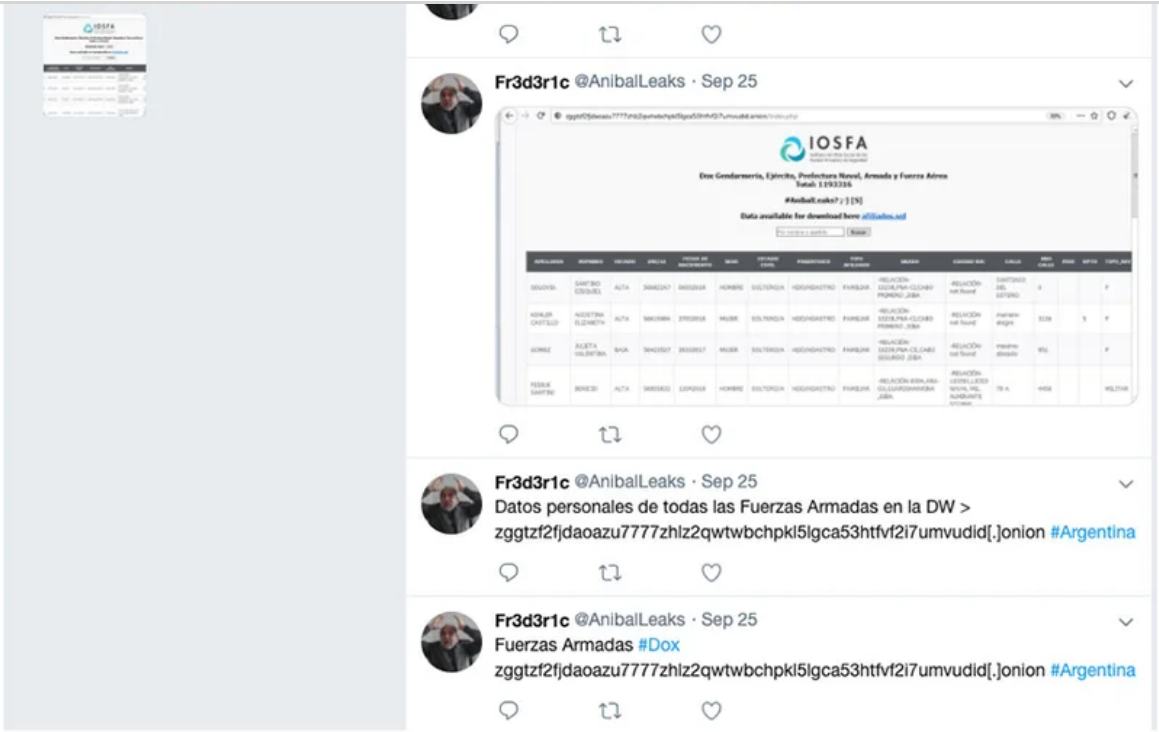
La filtración de los datos de la base del RENAPER revela que no cuenta con un sistema de alerta frente a consultas masivas

6

Un periodista de Estados Unidos contactó al hacker y le pidió datos de distintos DNI elegidos al azar. El hacker respondió con toda esa información.

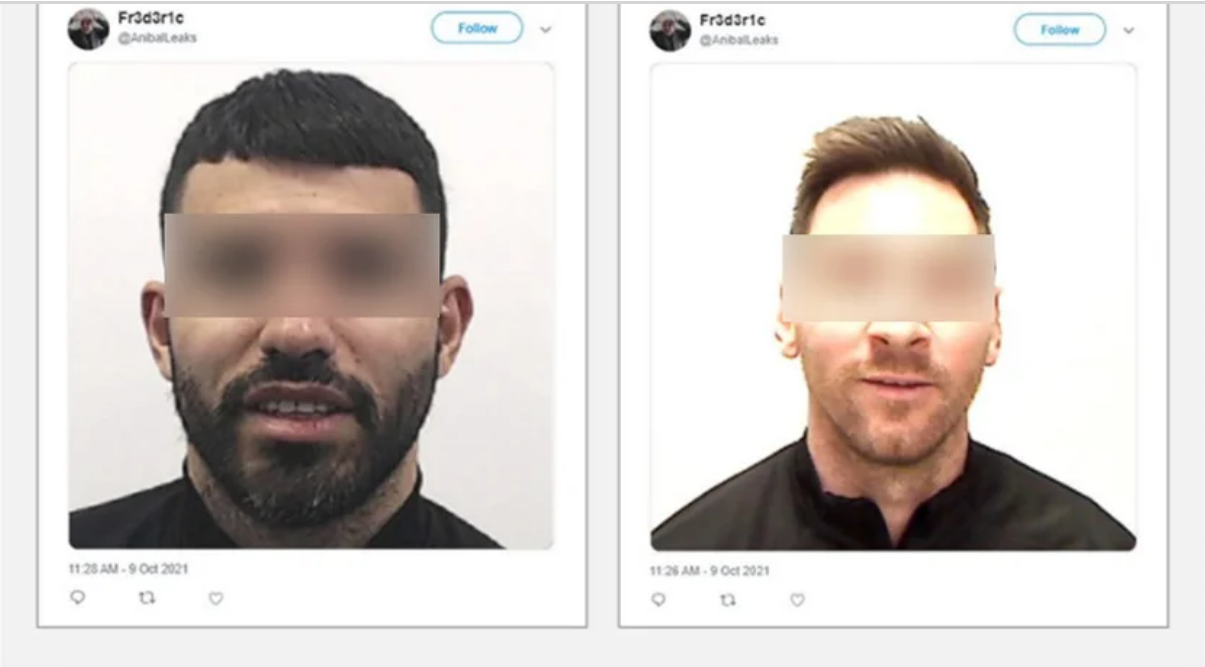
Este es uno de los principales

El **25 de septiembre** pasado, el hacker había filtrado a través de la misma cuenta de Twitter @AnibalLeaks la base de datos de la obra social de las Fuerzas Armadas (IOSFA), Gendarmería, Prefectura y el Ministerio de Defensa. Por esta filtración, se abrió una primera causa judicial que recayó en el Juzgado federal a cargo de la jueza María Eugenia Capuchetti, quien la delegó en el fiscal Eduardo Taiano.



El hacker publicitó en Twitter que accedió a la base de datos de IOSFA

A través de esa cuenta, cuya identidad remite al nuevo ministro de Seguridad y lleva su foto de perfil, pero con el apellido de la antecesora del ministro de Seguridad "**Fr3d3r1c**", se publicaron el **9 de octubre** fotos de DNI y datos personales de 44 argentinos con alta exposición pública. Entre ellos, las imágenes del presidente Alberto Fernández, Marcelo Tinelli, Gustavo Beliz, Juan Manzur, Santiago Cafiero, Oscar Parrilli, Máximo y Florencia Kirchner, Lionel Messi, Sergio Aguero, Elisa Carrió, Sandra Arroyo Salgado y Alberto Nisman, Jorge Lanata, Nelson Castro y Alfredo Leuco. También, las de **los ex jefes de la AFI macrista Gustavo Arribas y Silvia Majdalani**.

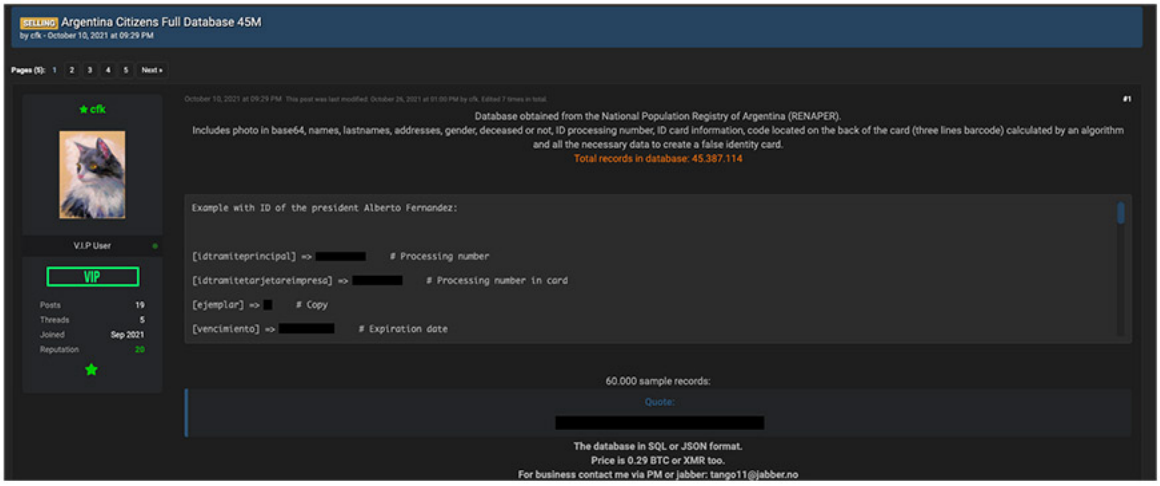


Images of Sergio Aguero (left) and Lionel Messi, tweeted by @AnibalLeaks (Image source: web.archive.org)

Algunas de las fotos de los DNI de los famosos filtradas por la cuenta @AnibalLeaks, hoy suspendida

Para esa misma fecha, el hacker puso a la venta en un foro de piratería el acceso a los datos personales de 45.387.114 argentinos por 17.000 dólares en bitcoins. “Vendo todo lo necesario para crear una identidad falsa”, aseguraba. Y publicó una dirección de contacto del servicio de mensajería Jabber.

A través de esta dirección, un periodista de Estados Unidos lo contactó y le solicitó datos de DNI elegidos al azar, que el hacker proveyó. Ese intercambio quedó reflejado en una nota de *The Record* y demostró que el autor del hackeo -que se especula es argentino- podría acceder, al azar, a los datos de cualquier persona que haya tramitado el DNI en el país.



El 10 de octubre último, **el hacker filtró la muestra de 60.000 registros a los que accedió Infobae**. Se trata de un archivo en formato "JSON", de 2,55 Gigabytes, con los siguientes campos: número de identificación personal, número de trámite, tipo de ejemplar, fecha de vencimiento del documento, emisión, nombre y apellido, sexo, fecha de nacimiento, CUIL, domicilio con código postal, barrio, municipio, ciudad, provincia y país, si la persona falleció o no, y la foto del DNI. Ningún campo contiene el número de teléfono ni fijo ni celular. Tampoco las huellas digitales. **La última fecha de renovación de documento que aparece en el registro es del 30 de septiembre. Esto revelaría que el hacker tuvo acceso a la base a fines de septiembre o principios de octubre.**

Hace 10 días, un argentino residente en Londres, Victor Atila Castillejo Arias, lo contactó y le pidió que demostrara que todavía tenía acceso a la base del Renaper. Para eso, le preguntó si le podía enviar sus propios datos personales, y el hacker le respondió con una copia de esos datos, junto con su foto del DNI.

El 19 de octubre un argentino residente en Londres reveló que contactó al hacker y éste le envió los datos personales a su pedido

conocida como LaGorraLeaks2.0, ocurrida en 2019.

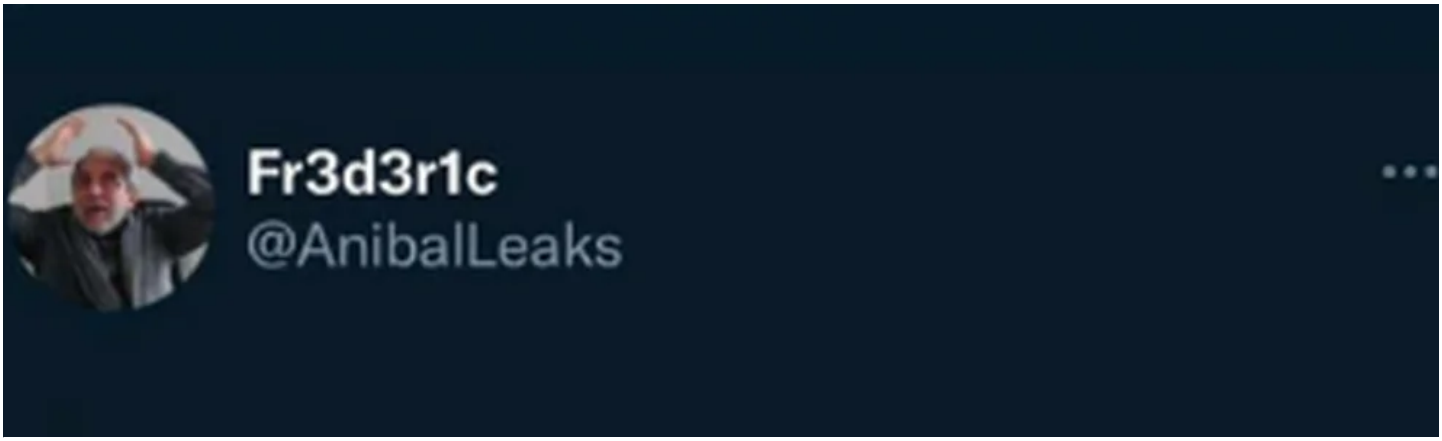
"El hacker es el mismo que filtró los datos de IOSFA. En la página que lo publica, **firmó con una [S] entre corchetes. [S] es el mismo que filtró los datos de la Policía Federal en 2019 en lo que se conoció como *LaGorraleaks2.0* y es el mismo que hackeó la cuenta de Patricia Bullrich en 2017** (cuando la entonces ministra apareció con posteos que decían "soy una borracha" y "Macri gato"), y los datos del Ministerio de Seguridad y la Policía Federal. Le hizo llegar los archivos a varios periodistas y luego los publicó", recordó Smaldone. "Con la filtración de *LaGorraleaks2.0* hizo un desastre porque reveló las identidades de todos los policías, incluidos los que estaban interviniendo en investigaciones de narcotráfico. **Ahora pasaron dos años, y el mismo hacker vuelve a actuar, poniendo a la venta los datos de todos los argentinos**", agregó Smaldone.

Esta semana, desde la **Unidad de Datos**, se buscó contactar al hacker a través de la dirección de Jabber publicada en el foro de piratería, pero no obtuvo respuesta.

¿Quién es el hacker?

Por ahora, la identidad del que robó los datos de identidad que tiene el Renaper de la totalidad de la población del país **sigue siendo un misterio.**

"Uno podría decir que el hacker hizo esto para mostrar la debilidad del sistema. **Pero podría haberlo hecho sin exponer las identidades de las personas, por ejemplo, no revelando los últimos dos números del número de trámite del DNI. Y además, quiere obtener una ganancia. No es un *hacktivista***, como se definió en la nota en una entrevista con un medio de Rosario. Es un delincuente, que busca un fin de lucro y está exponiendo la identidad de mucha gente. **Tendemos a bajarle la gravedad a los delitos cometidos a través de un teclado, y se puede causar un daño muy grave**", afirmó López.



Consecuencias

Desde el Renaper señalaron que las condiciones de seguridad cambiaron cuando se descubrió el robo de datos. Según fuentes oficiales consultadas por *Infobae*, **el organismo redujo al mínimo indispensable las consultas que se realizan a través de las credenciales del Ministerio de Salud**. Y cada uno de los dominios que ingresan por esa vía son revisados, para determinar si hubo algún consumo excepcional de datos. “Hay algunos casos sospechosos”, indicaron.

Esta filtración de información generó consecuencias no sólo para el Ministerio de Salud. “**A futuro, se restringirá al máximo la información de Renaper que no sea absolutamente indispensable”**, afirmaron. “Por ejemplo, si antes se pedía acceso a las fotos de los DNI, ahora se pedirá que la contraparte envíe sus fotos a Renaper para que se chequee si coincide con el DNI”, dijeron.

La Justicia ya investiga lo que sucedió, pero sin pistas firmes todavía. Hay, al menos, cuatro causas abiertas sobre las filtraciones, en tres Juzgados federales distintos: una realizada por la Policía Federal de oficio, otra por el propio Renaper, otra anterior por la filtración de datos de la obra social de las Fuerzas Armadas, y una cuarta realizada por el propio Ministerio de Salud.

En el medio, hay una disputa de competencia sobre si deben llevarse en forma unificada y cuál es la más avanzada, que deberá resolver la Cámara Federal. Hasta ahora, **los investigadores no tienen certezas sobre la extensión de la filtración y si alcanza a la base entera del Renaper o no. Tampoco cómo accedió quien robó los datos, o si fue una o más personas.**

El senador nacional de Juntos Pablo Daniel Blanco presentó la semana pasada un proyecto para solicitar al Poder Ejecutivo que brinde información, a través del Ministerio del Interior y el de Seguridad de la Nación, sobre **las fallas en la ciberseguridad del Renaper** y cuáles son las medidas adoptadas en relación a la pérdida de los datos**.**“Más allá de las circunstancias particulares del caso, el hecho ocurrido pone de manifiesto la **gran vulnerabilidad a la que se encuentran expuestos los ciudadanos** cuando las acciones u omisiones del gobierno se alejan de las prácticas profesionales que apliquen competencias de las personas y procedimientos orientados a la protección y promoción del bien común”.

La foto del DNI del gobernador Axel Kicillof, otras de las filtradas por la cuenta de @AnibalLeaks

argentino. Y la Justicia está enredada en un montón de causas y la Policía no lo encuentra", concluyó Smaldone.

¿Cómo se procesó la información?

La muestra de la filtración es un archivo JSON: un formato de texto sencillo para el intercambio de datos. Los datos se estructuraron en una hoja de cálculo. Las 60.000 filas del registro permitieron el análisis por fecha, apellido, lugar de residencia, sexo, fechas de nacimiento y de expiración del DNI.

Procesamiento de los datos: Daniela Czibener

Infografías: Marcelo Regalado

SEGUIR LEYENDO:

Renaper: investigan a ocho empleados por la filtración de datos, pero el Gobierno desmiente un hackeo

TEMAS RELACIONADOS

Renaper AnibalLeaks Hackeo Javier Smaldone Julio López

Últimas noticias LaGorraLeaks Números de DNI

ÚLTIMAS NOTICIAS

Los dardos de Ibarra tras la victoria de Boca: ironía por el partido Senior, la polémica con Zambrano y el Superclásico ante River

El entrenador xeneize habló en la conferencia luego del gran triunfo ante Atlético Tucumán que lo metió en la pelea por el campeonato. Qué consejo le dio al héroe Luca Langoni

Matt Damon sigue su recorrida por