Filtraron datos completos, como DNI, foto y número de trámite, pertenecientes al Registro Nacional de las Personas

14/10/2021

Una base de datos del Registro Nacional de las Personas (Renaper) se filtró y apareció a la venta en la Web. Además, una cuenta de Twitter que ya fue eliminada, @aniballeaks, compartió capturas de los DNI de varios famosos argentinos. El Renaper **confirmó la noticia pero aclaró que no se trató de un hackeo**.

El organismo, que depende del Ministerio del Interior, informó mediante un comunicado que **“se trató de un uso indebido de usuario o robo de la clave del mismo”**, y subrayó que “la base de datos no sufrió vulneración o filtración alguna de datos”.

La institución presentó una denuncia luego de detectarse que, a través del uso de claves otorgadas a organismos públicos, en este caso el Ministerio de Salud, “se filtraron imágenes como pertenecientes a trámites personales realizados en el Renaper”.

“Se detectó que esas 44 personas habían sido consultadas de manera completa desde una credencial del servicio del Ministerio de Salud. La mitad de esas, 18 o 19, fueron consultadas el mismo día, a la misma hora que se compartieron en Twitter”, explicaron a **TN Tecno** fuentes gubernamentales. También aclaron, en lenguaje informático, que para acceder a esos datos hacían falta “credenciales altas”. Dicho de otra forma, no pudo haberlo hecho un empleado raso.

El sábado 9 de octubre el Renaper tomó conocimiento de que un usuario de Twitter identificado con el nombre de @anibalLeaks, cuenta que fue denunciada y que actualmente se encuentra suspendida, había publicado **las imágenes de 44 individuos**, entre los cuales se encontraban funcionarios y personajes públicos. El programador Javier Smaldone compartió varios de los tuits de este perfil en su propia cuenta. Su propio DNI también fue viralizado.

Daniel Monastersky, abogado especialista en delitos informáticos, habló sobre la falla de seguridad y cómo debería actuar el organismo. “En el 2018 hay una comunicación de la Dirección de Protección de Datos en la que sugiere que la notificación de este tipo de hechos para que se tomen cartas en el asunto, respecto a **qué datos se comprometieron y detallar cómo se produce este tipo de filtraciones**”, explicó el letrado.

También citó al reglamento Europeo de protección de datos. “Si bien es una recomendación, no es exigible, hay cuestiones más técnicas que tiene que ver sobre qué implicancias tuvo.

Cualquiera de las personas implicadas puede realizar una denuncia y solicitar una investigación para ver si se contaba con las protecciones básicas a fin de evitar estas filtraciones", agregó Monastersky.

En esta oportunidad, **el propio Renaper ya avanzó con una denuncia penal** y envió información a los medios sobre el caso. El organismo tiene converios de interoperabilidad con diferentes organismos públicos, y uno de ellos es justamente el Ministerio de Salud, la fuente más clara para descubrir el origen de esta filtración.

"DNI Gate": uso indebido de la base del Renaper

Tras confirmar el hecho, el equipo de seguridad informática del Renaper realizó una consulta sobre las 44 personas involucradas "a fin de relevar los últimos consumos realizados mediante el uso del Sistema de Identidad Digital (SID) sobre dichos perfiles".

La investigación detectó que "19 imágenes habían sido consultadas en el exacto momento que eran publicadas en la red social Twitter **desde una conexión autorizada de VPN** (Virtual Private Network / Red Privada Virtual) entre el Renaper y el ministerio de Salud de la Nación, y que todas las imágenes habían sido consultadas recientemente desde esa misma conexión", según informó el organismo.

Desde esa conexión **se habrían realizado "varias consultas individuales a las bases de datos del Renaper** entre las 15:01 y las 15:55 mediante el servicio de validación de datos del SID, el cual, una vez invocados el DNI y sexo de la persona, devuelve a quien consulta toda la información impresa en el DNI, y que incluye imagen y otros datos personales, los cuales fueron subidos inmediatamente a la red social Twitter, sin el consentimiento del titular de los mismos", detalló el

comunicado.

Y agregó que luego de este análisis preliminar se descartó de plano un ingreso no autorizado a los sistemas, o una filtración masiva de datos del organismo, según pudieron confirmar los especialistas.

Se detectó, además, que **un usuario autorizado individual habría utilizado de forma indebida** para fines personales el servicio de validación de identidad a través de un certificado habilitado del Ministerio de Salud de la Nación, conectándose a través de la correspondiente VPN, con usuario y contraseña.

Filtración de datos de miembros de las Fuerzas Armadas y de Seguridad

A fines de septiembre información privada y sensible de miembros de las Fuerzas Armadas y de Seguridad de Argentina se filtró hacia la "dark web" y en varios foros de "piratas informáticos", reveló la consultora Privacy Affairs encargada de proveer asesoramiento destinado a proteger datos personales.

En IOSFA (Instituto de Obra Social de las Fuerzas Armadas y de Seguridad), emitieron un comunicado en el que reconocieron la filtración, no precisaron el número de afectados y negaron que se haya tratado de un ciberataque.

Captura de la supuesta filtración de datos de miembros de las Fuerzas Armadas y de Seguridad.

Según un reporte publicado en la página web de **Privacy Affairs**, "el 26 de septiembre de 2021 un usuario de un foro relacionado con la piratería afirmó poseer información confidencial de más de un millón de miembros de varias ramas e instituciones militares de Argentina". **Serían 1.193.316 en total.**

Fuente: TN