OSEP en la mira: un grupo hacker amenaza con una megafiltración de datos en la Argentina

30/03/2026

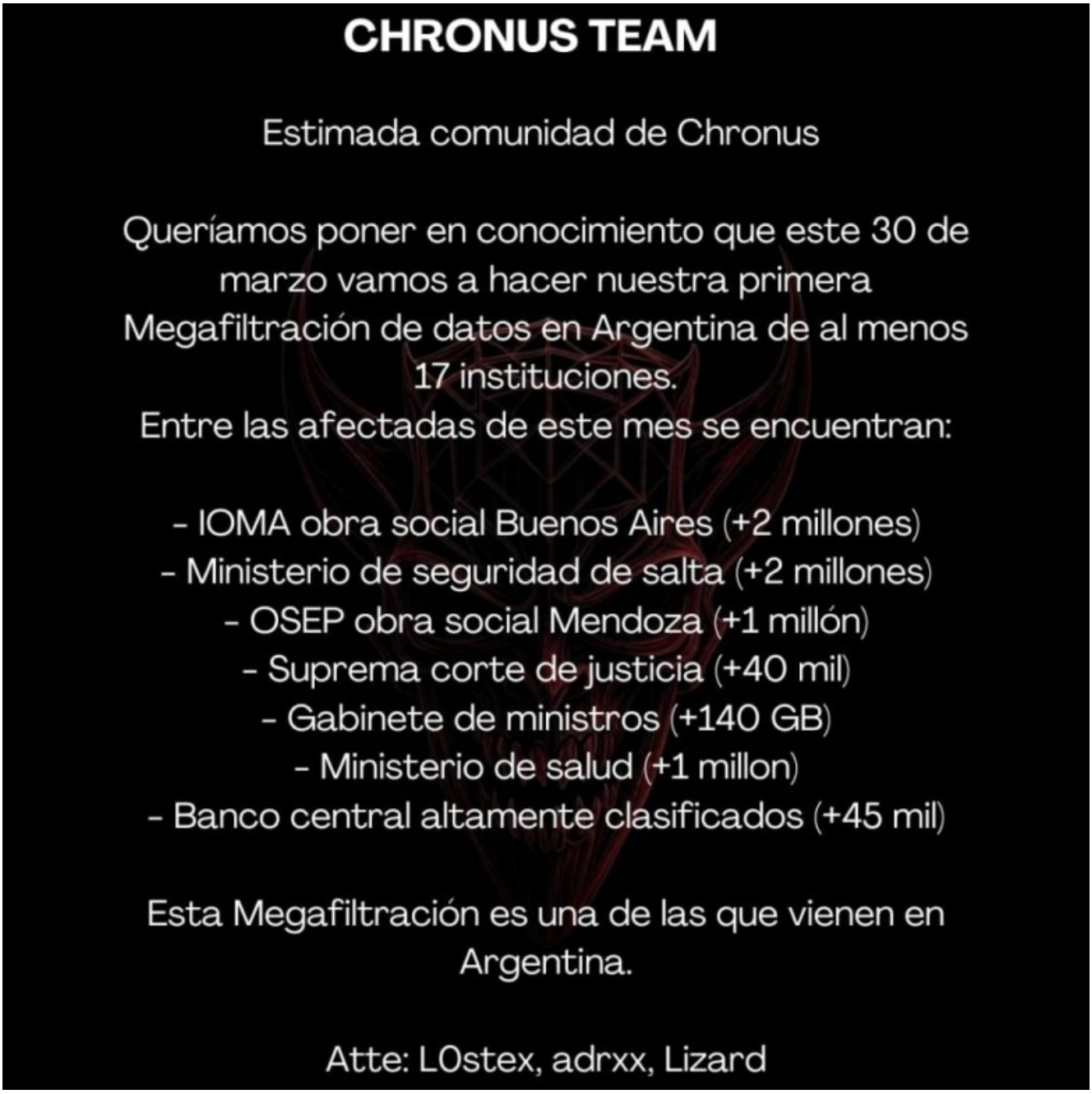
Con fondo negro, tipografía blanca y un tono desafiante, un mensaje comenzó a circular con fuerza en foros y canales vinculados al mundo **hacker**, y luego se extendió a las redes sociales. La advertencia es directa: *“Este 30 de marzo vamos a hacer nuestra primera megafiltración de datos en Argentina de al menos 17 instituciones”.*

La publicación está firmada por **Chronus Team**, un grupo hacktivista con antecedentes en América Latina, especialmente

en México, donde fue vinculado a filtraciones de datos en organismos públicos. Por el momento, **no hay confirmación oficial de intrusiones en Argentina** vinculadas a este anuncio.

El grupo enumera posibles objetivos y dimensiona el alcance con cifras:

- IOMA, la obra social de la provincia de Buenos Aires (+2 millones)
- Ministerio de Seguridad de Salta (+2 millones)
- *OSEP (+1 millón)*
- Corte Suprema (+40 mil)
- Jefatura de Gabinete (+140 GB)
- Ministerio de Salud (+1 millón)
- Banco Central (+45 mil)



En la lista aparece un organismo clave de Mendoza: la **Obra Social de Empleados Públicos (OSEP)**, que administra información sensible de cientos de miles de afiliados, incluyendo datos personales, registros de salud y detalles financieros.

De todas maneras, desde la obra social provincial indicaron que no existen registros de un hackeo a sus sistemas. *“Desmentimos esa información”*, aseguraron.

Qué es Chronus Team

Según especialistas en ciberseguridad, **Chronus Team no responde al perfil de una organización de espionaje altamente sofisticada.** Se trata de un clúster de activistas que opera con una lógica pragmática: detectan vulnerabilidades comunes —como credenciales reutilizadas, sistemas desactualizados o portales mal configurados—, acceden a la información y luego la exponen para maximizar el impacto público.

Ese impacto es el corazón de su estrategia. El grupo suele combinar el **robo de datos** con el *"defacement"*, una práctica que consiste en intervenir sitios web para modificar su contenido y dejar mensajes provocadores.

Su actividad documentada se concentra en México, donde se les atribuyen ataques a organismos de salud y sistemas fiscales. Investigaciones independientes reportan decenas de intrusiones confirmadas y **más de mil incidentes de seguridad** asociados a su ecosistema desde 2021.

Su estructura es otro rasgo distintivo: **no funcionan como una organización jerárquica**, sino como una identidad compartida bajo la que operan distintos actores. Alias como *L0stex, adrxx o Lizard* suelen aparecer firmando las acciones. Esta lógica descentralizada **dificulta su rastreo** por parte de las autoridades.

¿Amenaza real o propaganda?

La advertencia sobre Argentina encaja en un proceso de expansión regional del grupo, que ya ha registrado actividad en Brasil y Venezuela. De todos modos, **debe interpretarse con cautela.**

En el ecosistema hacktivista, este tipo de publicaciones también cumple una función propagandística: **puede anticipar una filtración real, exagerar capacidades o simplemente instalar una agenda de miedo.**

No hay evidencia pública que confirme que la megafiltración haya ocurrido, pero la inclusión de organismos argentinos —**y de la OSEP en particular**— vuelve a poner en foco la exposición de sistemas que gestionan información crítica.

Aun así, el efecto ya es concreto y el interrogante sigue abierto. En cualquier escenario, **Mendoza ya entró en el radar del cibercrimen regional.**

Fuente: El Sol – https://www.elsol.com.ar/mendoza/osep-en-la-mira-un-grupo-hacker-amenaza-con-una-megafiltracion-de-datos-en-la-argentina/