

La información sustraída equivale a 3.300 millones de fotos de alta calidad de un celular

# Así es el centro de súper computación chino que fue hackeado: robaron 10 Petabytes

**“La información hackeada al centro sería atractiva para los servicios de inteligencia de países adversarios”, dijo experto en ciberseguridad.**

JOAQUÍN RIVEROS

**D**atos clasificados como de alta seguridad, entre ellos, documentos de defensa y hasta planos de misiles fueron hackeados de una supercomputadora estatal china, ubicada en el National Supercomputing Center (NSCC, Centro Nacional de Supercomputación Chino), en lo que sería el mayor hackeo de información en dicho país, informó CNN.

Según la cadena, una muestra de los datos fue publicada el 6 de febrero pasado en una cuenta anónima del grupo de hackers llamado “Flaming-China”, de Telegram, donde se explicó que, entre otras cosas, contenía investigaciones de diversos campos, incluidos “ingeniería espacial, investigación militar, bioinformática, simulación de fusión y más”.

El 19 de marzo, el sitio especialista en ciberseguridad Netaskari había dado un adelanto de la noticia informada por CNN: “Cerca de dos meses atrás nosotros vimos un anuncio de venta en un foro de la Dark Web, por un hacker llamado “airborneshark1”. Él ofrecía 10 Petabytes de datos aparentemente extraídos del NSCC en Tianjin, una muestra de los cuales costaba US\$3.000”, señaló.

## ¿Qué es el NSCC?

Ubicado en Tianjin, al norte de China, el NSCC es un centro de infraestructura en el que se basa la capacidad de cómputo de alto rendimiento (HPC, por sus siglas en inglés) de China, con implicaciones directas en la investigación militar y científica



El NSCC es clave en la inteligencia militar China.

del país. Está ubicado en el “Tianjin Economic-Technological Development Area (TEDA), el corazón industrial del norte de China. Fue creado en 2009 y es uno de varios centros similares ubicados en las ciudades de Guangzhou, Shenzhen, Chengdu, Wuxi y Jinan. En él se encuentra el supercomputador Tianhe-1 A, uno de los primeros que sustentaron el macro manejo de datos chino y el Thiane-3, que según datos de la National University of Defense Technology, NUTD, (Universidad Nacional de Tecnología de la Defensa de China), tiene capacidades de exaescala (un trillón de cálculos por segundo) y es un activo de seguridad nacional Grado 4, el máximo del gigante asiático.

El centro entrega servicios de infraestructura a más de 6.000 clientes en China, incluidas agencias científicas y de defensa.

Su objetivo, desde que fue creado es impulsar la innovación en I+D, la modernización de la industria, el crecimiento empresarial y la digitalización de servicios gubernamentales. El centro está dirigido por la citada NUDT.

La institución está en la lista negra comercial del Departamento de Comercio de Estados Unidos debido a su vinculación con la industria militar. Esto le impide acceder a chips de última generación estadounidenses, prohibición que llevó a China a desarrollar opciones propias.

Expertos consultados por CNN que revisaron la información, señalaron que era auténtica y que incluía archivos en chino clasificados como secretos, con información técnica, simulaciones animadas y representaciones de equipos de defensa, incluyendo

bombas y misiles.

Mark Hofer, investigador en ciberseguridad y autor del sitio Netaskari, señaló a CNN que “la información hackeada al centro sería atractiva para los servicios de inteligencia de países adversarios. Solo ellos tienen la capacidad de analizarlos y obtener algo útil”, dijo. La información hackeada está vinculada a organizaciones de alto nivel, entre estas la Corporación de la Industria de la Aviación China, la Corporación de Aeronaves Comerciales de China y la Universidad Nacional de Tecnología de Defensa.

El volumen de datos hackeados está en torno a los 10 petabytes. Estos equivalen a 10.240 TB y 1 Terabyte a 1.024 Gigabyte (GB). A escala humana, 10 Petabytes equivale a 3.300 millones de fotos de alta calidad de un celular.