Noticias |**Estados Unidos**

La peor catástrofe de seguridad en la historia de la inteligencia estadounidense

Por Scott Shane , Nicole Perlroth y David E. Sanger

Jake Williams, un exintegrante de la unidad de "hackeo" de la Agencia de Seguridad Nacional
Credit Dustin Chambers para The New York Times

WASHINGTON — En abril, Jake Williams despertó en un hotel de Orlando, Florida, donde estaba a cargo de una sesión de capacitación. Al momento de revisar Twitter, Williams, un experto en

ciberseguridad, quedó consternado al descubrir que lo habían involucrado en una de las peores debacles de seguridad que haya sufrido la inteligencia estadounidense en su historia.

Williams había escrito en el blog de su empresa acerca de The Shadow Brokers, un misterioso grupo que de alguna manera había obtenido muchas herramientas de *hackeo* que utilizaba Estados Unidos para espiar a otros países. Ese día, la agrupación había respondido con una diatriba en Twitter. Williams era identificado —de manera correcta— como un exintegrante del grupo de *hackers* de la Agencia de Seguridad Nacional (NSA, por su sigla en inglés), Tailored Access Operations (Operaciones de Acceso a la Medida) o TAO, un trabajo del que él no había hablado en público. Después The Shadow Brokers lo dejó atónito porque divulgó detalles técnicos que dejaban claro que el grupo tenía conocimiento de operaciones de *hackeo* altamente clasificadas que él había dirigido.

La agencia de inteligencia más grande y hermética de Estados Unidos había sido infiltrada a profundidad.

"Tenían conocimiento operativo que no tenía ni la mayoría de mis colegas en las TAO", reconoció Williams, quien ahora trabaja en Rendition Infosec, la firma de ciberseguridad que fundó. "Sentí que me habían golpeado en el estómago. Quien había escrito eso era un infiltrado con mucho acceso o alguien que había robado una gran cantidad de información operativa".

El impacto que recibió Williams por el contrataque de The Shadow Brokers fue parte de un sismo mucho más intenso que ha sacudido a la NSA hasta la médula. Exfuncionarios y funcionarios en activo de la agencia aseguran que las divulgaciones de The Shadow Brokers —las cuales comenzaron en agosto de 2016— han sido catastróficas para la NSA, pues han generado cuestionamientos respecto de su capacidad para proteger poderosas ciberarmas y de su valor mismo para la seguridad nacional. La agencia, que es considerada líder mundial en lo que respecta a meterse en las redes de cómputo de sus adversarios, no pudo proteger su red.

"Esas filtraciones han ocasionado un daño significativo a nuestra inteligencia y capacidades en cibernética", afirmó Leon E. Panetta, exsecretario de Defensa y exdirector de la CIA. "El propósito fundamental de la inteligencia es ser capaz de penetrar de forma eficaz a nuestros adversarios para

recabar información vital. Por su naturaleza misma, lo anterior solo funciona si se mantiene el secreto y nuestros códigos están protegidos".

Después de quince meses de una investigación exhaustiva realizada por un brazo de contrainteligencia de la agencia, conocido como Q Group, y el FBI, los funcionarios aún no saben si la NSA fue víctima de un *hackeo* ejecutado de manera brillante —con Rusia como principal sospechosa—, del trabajo de un infiltrado o de ambas posibilidades. Desde 2015, tres empleados fueron arrestados por haber robado archivos clasificados, pero se teme que aún haya un infiltrado o incluso más de uno. Además, hay un consenso amplio en cuanto a que el daño que ha provocado The Shadow Brokers a la inteligencia estadounidense es mucho mayor que el causado por Edward J. Snowden, el excontratista de la NSA que en 2013 huyó con material clasificado.

La cascada de revelaciones que Snowden entregó a los periodistas y su postura pública desafiante tuvieron mucho más cobertura por parte de los medios de la que ha tenido esta nueva filtración. No obstante, Snowden divulgó palabras del código, mientras que The Shadow Brokers ha divulgado todo el código; si Snowden compartió lo que se podría describir como "planes de batalla", ellos han liberado las armas. Esas ciberarmas han sido recogidas por *hackers* de Corea del Norte y Rusia y ya las han utilizado para contratacar a Estados Unidos y sus aliados.