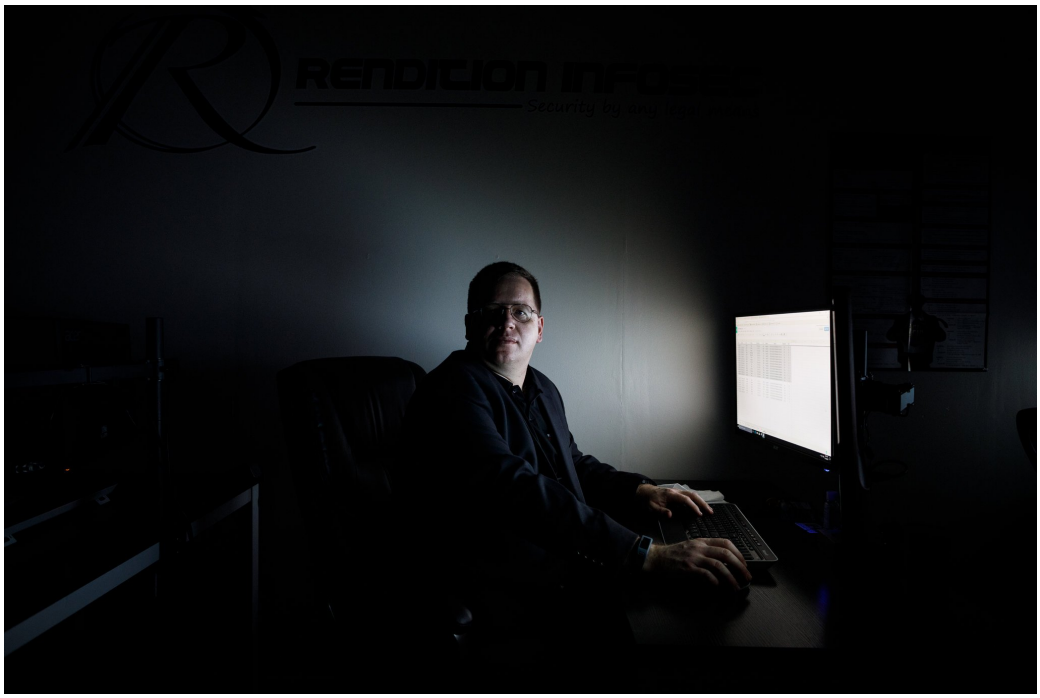
La peor catástrofe de seguridad en la historia de la inteligencia estadounidense

Por Scott Shane , Nicole Perlroth y David E. Sanger
New York Times, 14 de noviembre de 2017



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

Read in English

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.

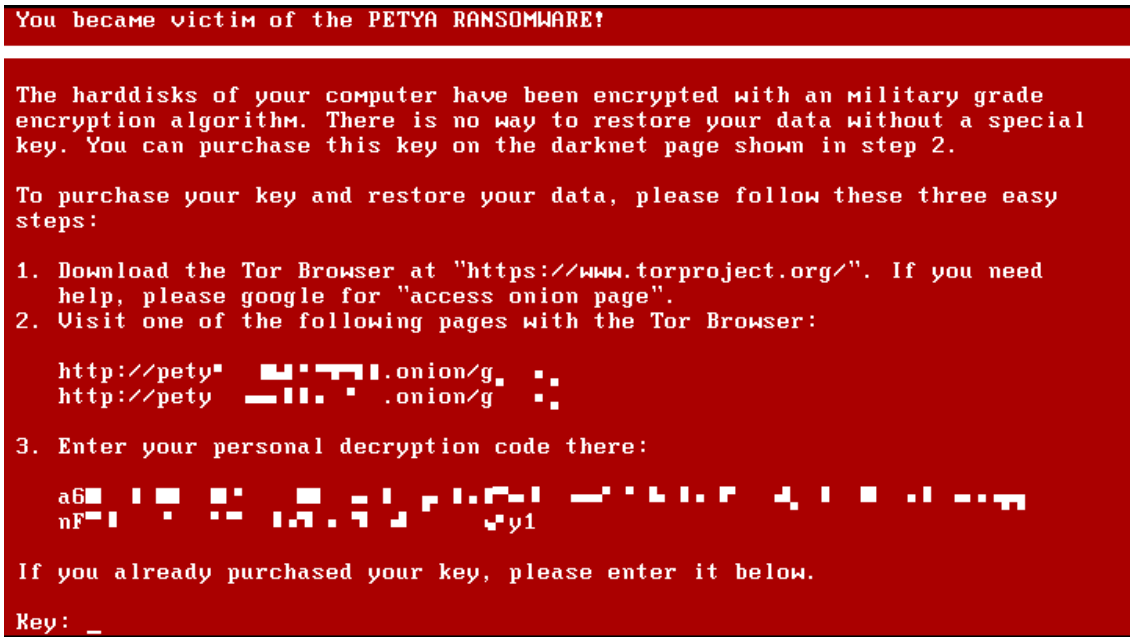
“Tenían conocimiento operativo que no tenía ni la mayoría de mis colegas en las TAO”, reconoció Williams, quien ahora trabaja en Rendition Infosec, la firma de ciberseguridad que fundó. “Sentí que me habían golpeado en el estómago. Quien había escrito eso era un infiltrado con mucho acceso o alguien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



Una captura de pantalla tomada cuando el programa de secuestro afectó sistemas en todo el mundo el verano pasado. El gobierno ucraniano publicó la imagen en su perfil oficial de Facebook.

Dentro de las oficinas de la agencia en Maryland y sus campus en todo el país, empleados de la NSA han pasado por polígrafos y han sido suspendidos como parte de la cacería de los desertores que se han aliado con The Shadow Brokers. Todavía se sigue remplazando una buena parte del ciberarsenal de la agencia, lo cual ha reducido las operaciones. Ha decaído la moral y los ciberespecialistas con experiencia están dejando la agencia para irse a trabajos mejor pagados, entre ellos, puestos en firmas que defienden redes de cómputo de los intrusos que utilizan las herramientas filtradas de la NSA.

“Es un desastre en muchos niveles”, afirmó Williams. “Es vergonzoso que las personas responsables de estos actos no hayan sido llevadas ante la justicia”.

Rusia es la primera sospechosa de una hemorragia paralela de *hackeo* de herramientas y documentos secretos del Centro de Ciberinteligencia de la CIA que se ha publicado en el sitio web de WikiLeaks semana tras semana desde marzo bajo los nombres de Vault7 y Vault8. Esta filtración tampoco se ha resuelto. La revelación conjunta de secretos digitales de agencias que han invertido una gran cantidad de recursos para prevenir este tipo de filtraciones está generando cuestionamientos profundos.

¿Los *hackers* y los “filtradores” volvieron obsoleto el secreto? ¿La inteligencia rusa sencillamente ha superado a la estadounidense después de ingresar a los rincones mejor guardados de su gobierno? ¿La fuerza laboral de miles de espías jóvenes expertos en tecnología alguna vez podrá ser inmune a las filtraciones?

Las oficinas de la NSA en Fort Meade en Maryland Jim Lo Scalzo/European Pressphoto Agency

Famosa desde hace mucho tiempo por ser una agencia que gusta de escuchar tras las paredes, a la NSA ha el *hackeo* le ha resultado una forma especialmente productiva de espionaje en contra de objetivos extranjeros.

La recopilación de información suele ser automatizada por medio de implantes de programas maliciosos —código de cómputo diseñado para encontrar material de interés—, que se instalan en el sistema del blanco durante meses o incluso años, durante los cuales envía archivos a la NSA. El mismo implante puede ser utilizado para muchos propósitos: robar documentos, ingresar a correos electrónicos, cambiar datos de forma sutil o convertirse en la plataforma de lanzamiento de un ataque.

La operación de las TAO que tuvo más éxito público fue en contra de Irán y la llamaron "Juegos Olímpicos"; en esta, los implantes en la red de la planta nuclear de Natanz provocaron que se autodestruyeran las centrifugadoras que enriquecían el uranio. Las TAO también fueron cruciales en los ataques en contra del Estado Islámico y de Corea del Norte.

The Shadow Brokers se apoderó precisamente de este ciberarsenal y lo comenzó a utilizar.

Como sucede cuando la policía estudia la forma de operar de los ladrones y la cantidad de pertenencias robadas, los analistas de la NSA han intentado descifrar

qué se llevó The Shadow Brokers. Ninguno de los archivos filtrados es posterior a 2013: un alivio para los funcionarios de la agencia que están evaluando el daño. No obstante, sí hay entre ellos una gran cantidad de datos recopilados por las TAO, incluidos tres "discos de operaciones" —el término de las TAO para los conjuntos de herramientas— que contenían el software que sortea los cortafuegos de las computadoras, penetra Windows y allana los sistemas Linux que suelen utilizar los teléfonos Android.

La evidencia demuestra que The Shadow Brokers obtuvo el conjunto de herramientas intacto, lo cual sugiere que un infiltrado simplemente logró robarse una memoria portátil y salir caminando de las instalaciones.

Sin embargo, los otros archivos que obtuvo The Shadow Brokers no están relacionados con los discos de operaciones y parece que se obtuvieron en distintos momentos.

Algunos funcionarios dudan que The Shadow Brokers haya obtenido todo *hackeando* a la agencia más segura del gobierno de Estados Unidos, razón por la cual están buscando infiltrados. No obstante, algunos de los *hackers* de las TAO creen que algunos atacantes hábiles e insistentes pudieron haber superado a las defensas de la NSA porque, como lo dejó claro uno de ellos: "Sé que lo hemos hecho igual con otros países".

El trauma que dejó Snowden llevó a la inversión de millones de dólares en nueva tecnología y regulaciones más estrictas para contrarrestar la que el gobierno llama "la amenaza interna". No obstante, los empleados de la NSA aseguran que, al tener miles de empleados y la capacidad de almacenar bibliotecas de datos en dispositivos que pueden caber en un llavero, es imposible prevenir que la gente salga de las oficinas con secretos en los bolsillos.

Debido a que la unidad de *hackeo* de la NSA ha crecido de forma tan vertiginosa durante la última década, las filas de infiltrados potenciales han aumentado hasta los cientos. La confianza se ha erosionado porque cualquiera que tenga acceso al código filtrado es visto como un posible culpable.

"¿Durante cuánto tiempo más seguirá habiendo fugas de información?", preguntó un exempleado de las TAO. "La agencia no sabe cómo detenerlo… ni siquiera de 'qué' se trata".

Williams afirmó que podrían pasar años antes de que se comprenda "todo el efecto secundario" de la filtración de The Shadow Brokers. Incluso el arresto del responsable de las filtraciones podría no detenerlas, explicó, pues los perpetradores sofisticados podrían haber creado un "dispositivo automático" para divulgar todos los archivos restantes en caso de que fueran capturados.
"Es evidente que estamos frente a gente que cuenta con conocimiento sobre seguridad operativa", mencionó. "Los están persiguiendo todas las fuerzas del orden y todos los sistemas de inteligencia, y aun así no han sido capturados".