



El Departamento de Justicia de Estados Unidos, anunció hoy cuatro cargos contra cuatro hackers militares chinos que supuestamente estaban detrás de la [violación de datos de Equifax](#), que expuso los datos personales y financieros de casi 150 millones de estadounidenses.

En una conferencia de prensa conjunta celebrada hoy con el Fiscal General William Barr, y el director adjunto del FBI, David Bowdich, los [funcionarios del Departamento de Justicia](#) calificaron la campaña de piratería patrocinada por el estado como el mayor caso de hacking jamás descubierto de este tipo.

Los cuatro acusados, Wu Zhiyong (吴志勇), Wang Qian (王倩), Xu Ke (徐可) y Liu Lei (刘磊), también fueron acusados por su participación en piratería y robo de secretos comerciales, propiedad intelectual e información confidencial de otras empresas estadounidenses en los últimos años.

En septiembre de 2017, la agencia de informes crediticios Equifax, reveló que se había convertido en víctima de un ataque cibernético masivo que dejó datos altamente sensibles de casi la mitad de la población estadounidense en manos de piratas informáticos.

Los hackers comprometieron los servidores de Equifax al utilizar una vulnerabilidad crítica en Apache Struts Web Framework, que la compañía olvidó parchear a tiempo aún cuando una versión segura actualizada del software estaba disponible.

«Utilizaron este acceso para realizar el reconocimiento del portal de disputas en línea de Equifax y para obtener credenciales de inicio de sesión que podrían usarse para navegar aún más por la red de Equifax. Los acusados pasaron varias semanas ejecutando consultas para identificar la estructura de la base de datos de Equifax y buscando información sensible e identificable dentro del sistema Equifax», dijo el Departamento de Justicia.

«Una vez que accedieron a los archivos de interés, los conspiradores almacenaron



*la información robada en archivos de salida temporales, comprimieron y dividieron los archivos, y finalmente pudieron descargar y filtrar los datos de la red de Equifax a computadoras fuera de Estados Unidos. En total, los atacantes realizaron aproximadamente 9000 consultas en el sistema de Equifax, obteniendo nombres, fechas de nacimiento, entre otros datos».*

Los funcionarios del Departamento de Justicia afirmaron que el FBI comenzó la investigación hace dos años, con solo 40 direcciones IP involucradas en los ataques que llevaron a la agencia a los cuatro miembros del 54° Instituto de Investigación del Ejército Popular de Liberación.

*«Los acusados tomaron medidas para evadir la detección durante la intrusión, como se alega en la acusación. Enrutaron el tráfico por medio de aproximadamente 34 servidores ubicados en casi 20 países para ofuscar su verdadera ubicación, utilizaron canales de comunicación encriptados dentro de la red de Equifax para combinar con la actividad normal de la red, y borraron los archivos comprimidos y los archivos de registro a diario como un esfuerzo por eliminar los registros de su actividad»,* agregó el departamento.

Esta no es la primera vez que Estados Unidos acusa a oficiales de inteligencia chinos por piratería informática y espionaje cibernético. En 2014, se anunciaron cargos similares contra cinco oficiales militares chinos por piratería informática y espionaje cibernético contra distintas compañías estadounidenses.

Además, Estados Unidos también acusó a los otros dos hackers chinos en 2015 por una violación masiva de datos en la que los hackers robaron la información personal de alrededor de 80 millones de clientes de la compañía de seguros de salud Anthem.