Capital One, la quinta institución bancaria y emisora de tarjetas de crédito más grande de Estados Unidos, sufrió recientemente una violación de datos que expuso la información personal de más de 100 millones de solicitantes de tarjetas de crédito en el país y 6 millones en Canadá.

Dicha violación de datos ocurrió el 22 y 23 de marzo de este año, y permitió a los atacantes robar información de clientes que habían solicitado una tarjeta de crédito entre 2005 y 2019, según informó Capital One.

Sin embargo, el incidente se propagó públicamente después del 19 de julio, cuando un pirata informático publicó la información acerca del robo en su cuenta de GitHub.

El FBI arrestó al hacker involucrado

El FBI arrestó a Paige Thompson, un sujeto de 33 años, ex ingeniero de software de Amazon Web Services, que trabajó para un contratista de Capital One de 2015 a 2016. Referente a la violación de datos, ayer por la mañana se le confiscaron dispositivos de almacenamiento que contenían una copita de los datos robados.

Thompson compareció el lunes en el Tribunal de Distrito de Estados Unidos y fue acusado por fraude y abuso informático, que tiene como pena hasta 5 años de prisión y una multa de 150 mil dólares. Se programó una audiencia para el 1 de agosto de este año.

Según los documentos judiciales, Thompson supuestamente explotó un firewall mal configurado en el servidor en la nube de Amazon Web Services de Capital One y robó más de 700 carpetas con datos almacenados en el servidor en algún momento de marzo.

> *«Capital One alertó rápidamente a las fuerzas del orden público sobre el robo de datos, lo que permitió al FBI rastrear la intrusión. Elogio a nuestros socios encargados de hacer cumplir la ley que están haciendo todo lo posible para determinar el estado de los datos y asegurarlos»*, dijo el fiscal Moran.

Cabe señalar que Amazon Web Services no se vio comprometido de ninguna forma, ya que el presunto hacker obtuvo acceso al servidor en la nube debido a la configuración incorrecta de Capital One y no por medio de una vulnerabilidad en la infraestructura de Amazon.

Cantidad de clientes e información afectados

Los datos comprometidos incluyen alrededor de 140 mil números de seguridad social y 80 mil números de cuentas bancarias vinculadas a clientes de Estados Unidos, además de 1 millón de números de seguridad social canadienses.

Además, algunos nombres de clientes, direcciones, fechas de nacimiento, puntajes de crédito, límites de crédito, saldos, historial de pagos e información de contacto también resultaron entre la información comprometida.

Sin embargo, en un comunicado publicado este lunes, Capital One afirmó a sus clientes que *«no se comprometieron los números de cuenta ni de tarjetas de crédito o credenciales de inicio de sesión»,* y que más del 99% de los números de seguro social que la compañía tiene en el archivo no se vieron afectados.

> *«Capital One solucionó de inmediato la vulnerabilidad de configuración que este individuo explotó y rápidamente comenzó a trabajar con la policía federal. El FBI arrestó a la persona responsable. Según nuestro análisis hasta la fecha, creemos que es poco probable que la información haya sido utilizada para fraude o difusión por esta persona»*, dijo Capital One.

La compañía también aseguró que notificará a los clientes afectados y proporcionará servicios gratuitos de monitoreo de crédito a los afectados.