



En caso de que hayas utilizado tu tarjeta de crédito o débito en las cadenas de restaurante Drive-Rally en los últimos 3 años, debes solicitar a tu banco que bloquee tu tarjeta inmediatamente.

Checkers, una de las mayores cadenas de restaurantes de autoservicio en Estados Unidos, reveló ayer una violación masiva de datos de larga duración que afectó a un número desconocido de clientes en 103 ubicaciones de Checkers y Rally, siendo casi el 15% de sus restaurantes.

Los restaurantes afectados, de los que se robaron datos como nombres, direcciones y fechas de exposición, residen en 20 estados de Estados Unidos, incluyendo Florida, California, Michigan, Nueva York, Nevada, Florida, Alabama, entre otros.

Después de conocer un «*problema de seguridad de datos relacionado con maleare*» en algunas ubicaciones de Checkers y Rally, la compañía inició una extensa investigación que reveló que piratas informáticos desconocidos lograron plantar malware en sus sistemas de punto de venta (PoS) en 103 establecimientos.

El malware PoS fue diseñado para recopilar información almacenada en la banda magnética de las tarjetas de pago, incluido el nombre del titular de la tarjeta, número de tarjeta, código de verificación y fecha de vencimiento.

Sin embargo, la compañía aseguró que la investigación no encontró pruebas que sugirieran que los piratas informáticos se fugaron con información adicional perteneciente a los titulares de tarjetas afectados, y que «*no todos los invitados que visitaron los restaurantes incluidos en la lista*» se vieron afectados por la violación.

Estas son las supuestas fechas de exposición de los restaurantes afectados:

- Un restaurante en California tenía instalado en su sistema el malware PoS en diciembre de 2015, que capturaba continuamente la información de las tarjetas de los clientes hasta marzo de 2018.



- Dos restaurantes, uno en California y otro en Florida, tuvieron una puerta trasera con el malware PoS en 2016, que permitió a los hackers robar remotamente hasta 2018 y 2019 respectivamente.
- Cuatro restaurantes en cuatro estados diferentes se infectaron en 2017 y permanecieron infectados entre inicios de 2018 y 2019.
- Los restaurantes restantes fueron infectados en 2018 y se mantuvieron así hasta inicios de 2019.

La cadena de restaurantes aseguró a sus clientes que la compañía trabajó estrechamente con los expertos de seguridad de datos de terceros para contener y eliminar el malware al descubrir el incidente de seguridad.

Además, la compañía también está *«trabajando con las autoridades federales encargadas de hacer cumplir la ley y coordinándose con las compañías de tarjetas de pago en sus esfuerzos por proteger a los titulares de las tarjetas. Sigue tomando medidas para mejorar la seguridad de los sistemas de Checkers y Rally para evitar este tipo de problemas»*.

La compañía recomienda a los clientes que revisen sus estados de cuenta, soliciten un informe de crédito e informen cualquier incidente sospechoso a la Comisión Federal de Comercio.