Landry´s, una popular cadena de restaurantes en Estados Unidos, anunció un ataque de malware en sus sistemas de punto de venta (PoS), que permitió a piratas informáticos robar la información de la tarjetas bancarias de los clientes.

La cadena cuenta con más de 600 bares, restaurantes, hoteles, casinos, tiendas de alimentos y bebidas con más de 60 marcas diferentes como Landry´s SeaFood, Chart House, Saltgrass Steak House, Claim Jumper, Morton´s The Steakhouse, Mastro´s Restaurants y Rainforest Cafe.

Según la notificación de incumplimiento publicada esta semana, el malware fue diseñado para buscar y probablemente robar datos confidenciales de tarjetas de crédito de clientes, incluyendo números de tarjetas, fechas de vencimiento, códigos de verificación y en algunos casos, nombres de titulares.

El malware PoS infectó terminales de punto de venta en todas las ubicaciones de Landry, pero, debido a la tecnología de cifrado de extremo a extremo utilizada por la compañía, los atacantes no pudieron robar datos de tarjetas de pago de las tarjetas robadas en sus restaurantes.

Sin embargo, los puntos de venta de Landry también utilizan *«sistemas de ingreso de pérdidas con un lector de tarjetas conectado para que los camareros ingresen los pedidos de la cocina y el bar para pasar las tarjetas de recompensa de Landry´s Select Club»,* lo que permitió a los atacantes robar con éxito los datos de pago de los clientes *«en circunstancias excepcionales»* cuando los camareros les robaron tarjetas de pago por error.

La cadena de restaurantes no especuló cuántos clientes pueden haber sido afectados, pero está *«notificando a los clientes que en raras circunstancias, parece que los camareros robaron por error en los dispositivos utilizados para ingresar pedidos de cocina y bar, que son dispositivos diferentes de los terminales de punto de venta utilizados para el procesamiento de pagos»*, dice la notificación de incumplimiento.

> *«El malware buscó datos de seguimiento (que a veces tiene el nombre del titular de la tarjeta además del número de tarjeta, la fecha de vencimiento y el código de verificación interno) leídos de una tarjeta de pago después de que se deslizó en los sistemas de ingreso de pedidos. En algunos casos, el malware solo identificó la parte de la banda magnética que contenía información de la tarjeta de pago sin el nombre del titular de la tarjeta».*

Según la compañía, el malware de PoS escanó de forma activa sus sistemas entre el 13 de marzo de 2019 y el 17 de octubre de 2019, en busca de tarjetas magnéticas, y en algunos lugares, es posible que se haya instalado el 18 de enero de 2019.

> *«Durante la investigación, eliminamos el malware e implementamos medidas de seguridad mejoradas, y estamos brindando capacitación adicional para los camareros».*