Las plataformas de pedido de restaurantes, MenuDrive, Harbortouch e InTouchPOS, fueron el objetivo de dos campañas de desnatado de Magecart que resultaron en el compromiso de al menos 311 restaurantes.

Las tres infracciones llevaron al robo de más de 50,000 registros de tarjetas de pago de los restaurantes infectados y publicados para la venta en la Deep Web.

> *«Las plataformas de pedidos en línea MenuDrive y Harbortouch fueron blanco de la misma campaña de Magecart, lo que resultó en infecciones de skimmer electrónico en 80 restaurantes que usaban MenuDrive y 74 que usaban Harbortouch»,* dijo la compañía de seguridad cibernética Recorded Future.

> *«InTouchPOS fue el objetivo de una campaña de Magecart separada y no relacionada, lo que resultó en infecciones de e-skimmer en 157 restaurantes que usaban la plataforma».*

Los actores de Magecart tienen un historial de infectar sitios web de comercio electrónico con skimmers de JavaScript para robar datos de tarjetas de pago, información de facturación y otra información de identificación personal (PII) de los compradores en línea.

Se cree que el primer conjunto de actividades comenzó alrededor del 18 de enero de 2022 y siguió hasta que el dominio malicioso utilizado en la campaña fue bloqueado el 26 de mayo. La campaña InTouchPOS, por otro lado, permaneció activa desde el 12 de noviembre de 2021.

Cabe mencionar que el dominio de exfiltración de datos utilizado en las infecciones de MenuDrive y Harbortouch también fue identificado por la Oficina Federal de Investigaciones (FBI) de Estados Unidos en una alerta flash de mayo de 2022.

Los ataques implican la inserción de código PHP malicioso en las páginas de pago en línea de las empresas aprovechando vulnerabilidades de seguridad conocidas en los servicios para raspar y transmitir los datos del cliente a un servidor bajo el control del atacante.

La idea es que al apuntar a las plataformas de pedidos en línea, puede conducir a un escenario en el que incluso cuando se ataca una sola plataforma, las transacciones de docenas o incluso cientos de restaurantes pueden verse comprometidas, lo que permite que *«los ciberdelincuentes roben grandes cantidades de datos de tarjetas de pago de los clientes desproporcionado con respecto a la cantidad de sistemas que realmente piratean».*

El desarrollo es importante por varias razones. Primero, las intrusiones son una desviación del objetivo tradicional del actor de amenazas de la plataforma de comercio electrónico Magento, un hecho ejemplificado por el aumento en los ataques de skimmer dirigidos a un complemento de WordPress llamado WooCommerce.

Además, sirve para resaltar cómo las campañas de Magecart ahora están destacando a los pequeños restaurantes locales que dependen de software de terceros de servicios de pedidos en línea menos reconocidos en lugar de diseñar sus propias páginas web de pago, ampliando efectivamente el grupo de vectores de ataque.

> *«Las plataformas de pedidos centralizados que atienden a múltiples comerciantes ofrecen una oportunidad única para que los actores de amenazas de Magecart recopilen PII de los clientes y datos de tarjetas de pago. El creciente interés de los ciberdelincuentes en apuntar a las plataformas de pedidos en línea representa una nueva dimensión de riesgo para los restaurantes»*, dijeron los investigadores.