El procesador de pagos VISA asegura que los comerciantes norteamericanos que operan estaciones de servicio y bombas de gas, enfrentan una serie de ataques de grupos de hackers que desean implementar malware de punto de venta (PoS) en sus redes.

En dos alertas de seguridad publicadas en noviembre y diciembre, respectivamente, VISA dijo que su equipo de seguridad investigó al menos cinco incidentes de este tipo.

La compañía asegura que los grupos de delitos cibernéticos llevaron a cabo ataques con el objetivo principal de obtener acceso a las redes de comerciantes de dispensadores de combustible, donde instalaron malware POS.

El malware de punto de venta funciona al raspar de forma continua la RAM de una computadora para obtener lo que parecen datos de la tarjeta de pago sin cifrar, que recopila y luego carga en un servidor remoto.

El equipo VISA Payment Fraud Disruption (PFD), asegura que los grupos de delitos cibernéticos parecen haber encontrado un punto débil en cómo funcionan las estaciones de servicio y los operadores de bombas de gas.

Si bien las terminales de punto de venta en tiendas de algunos comerciantes pueden admitir transacciones con chips, la mayoría de los lectores de tarjetas instalados en bombas de gas no lo hacen.

Estos lectores de tarjetas de bombas de gas siguen funcionando con la tecnología más antigua que solo puede leer los datos de pago de la banda magnética de la tarjeta.

Los datos de estos lectores de tarjetas se envían sin cifrar a la red principal de la estación de servicio, donde los delincuentes se dieron cuenta de que pueden interceptarla.

VISA documentó infracciones en dos comerciantes de dispensadores de combustible en una alerta de seguridad de noviembre de 2019, y otras tres infracciones en una alerta de diciembre de 2019. Las dos alertas resaltan un nuevo objetivo y modus operandi para los

grupos de hackers.

Los ataques contra comerciantes de dispensadores de combustible comenzaron durante el verano, según informes de VISA. Dos de los cinco ataques estaban vinculados a una operación conocida de cibercrimen conocida como FIN8.

VISA aseguró que las formas más fáciles para que los comerciantes de dispensadores de combustible protejan a los clientes, es encriptar los datos de la tarjeta mientras se transfieren por medio de una red o almacenarse en la memoria o cambiar a una política de aceptación de tarjetas con chip.

> *«Los comerciantes de dispensadores de combustible deben tomar nota sobre esta actividad e implementar dispositivos que admitan chips siempre que sea posible, ya que esto reducirá significativamente la probabilidad de estos ataques»*, dijo VISA.

Los comerciantes de combustible tienen hasta octubre de 2020 para implementar lectores de tarjetas compatibles con chips en sus bombas de gas. A partir de octubre de 2020, VISA informó que la responsabilidad por cualquier fraude de tarjetas pasaría de los emisores de tarjetas a los comerciantes, lo que probablemente motivará a muchos operadores a actualizar sus lectores de tarjetas de bomba de gas. Hasta entonces, muchos siguen siendo vulnerables a los ataques cibernéticos.