Las gasolineras son un objetivo para los hackers, advierte Visa

Una reciente alerta de seguridad de Visa detalla cómo los grupos de piratas informáticos tienen como objetivo las gasolineras para robar datos de tarjetas bancarias.

En el verano de 2019, la interrupción de fraude de pago (PFD) de Visa identificó tres ataques únicos dirigidos a los sistemas de puntos de venta que probablemente fueron llevados a cabo por sofisticados grupos de ciberdelincuentes. Dos de los ataques se llevaron a cabo en gasolineras de Estados Unidos.

Visa advierte que ha visto un aumento de los ataques a los puntos de venta contra los comercios de surtidores de combustible, y es probable que estos minoristas sean un objetivo cada vez más atractivo para los grupos de ciberdelincuencia, según el proveedor de pagos globales.

La razón es la falta de tecnología de aceptación segura como EMV y tokenización, y el incumplimiento del PCI DSS.

Los grupos de hacking como FIN8 están explotando activamente las vulnerabilidades de las redes de puntos de venta de las gasolineras para escatimar los datos de las tarjetas sin necesidad de realizar modificaciones en los propios surtidores.

En uno de los incidentes, Visa descubrió cómo los piratas informáticos enviaron por primera vez un correo electrónico de phishing a un empleado. El correo electrónico contenía un enlace malicioso que, al ser pulsado, instalaba un troyano de acceso remoto en la red que permitía el acceso a la misma. Una vez que se accedió con éxito al entorno del punto de venta, se desplegó un rascador de memoria de acceso aleatorio (RAM) en el sistema del punto de venta para recoger los datos de las tarjetas de pago.

Los clientes pueden evitar el uso de sus tarjetas de crédito en los lectores de banda magnética pagando en efectivo o utilizando una aplicación de pago en una gasolinera, según los defensores de los consumidores.

Visa advierte que "sofisticados grupos de amenaza han identificado a los comerciantes de surtidores de combustible como un objetivo atractivo para obtener datos de rastreo".

Entre las recomendaciones emitidas por Visa a los minoristas se encuentran: Emplear los IOCs contenidos en el informe, asegurar el acceso remoto con una contraseña fuerte, habilitar las

tecnologías EMV, proporcionar a cada usuario administrador sus propias credenciales de usuario, activar el análisis de comportamiento sobre el antimalware, monitorear el tráfico de la red y mantener un programa de administración de parches.

En caso de sufrir una infracción confirmada o sospechada, consulte el documento de Visa What to do if Compromised (WTDIC), publicado en octubre de 2019.