LITORALPRESS

Fecha: 30-05-2024
Medio: Las Últimas Noticias
Supl. : Las Últimas Noticias
Tipo: Noticia general
Título: Detectan sistema contactless para clonar tarjetas en Cajeros automáticos

Pág. : 4
Cm2: 723,8

Tiraje: 91.144
Lectoría: 224.906
Favorabilidad: No Definida

"Los dispositivos colocados leen los chips", afirma inspector de la PDI

Detectan sistema contactless para clonar tarjetas en cajeros automáticos

El fraude proviene de Córdoba, Argentina, y captura la información bancaria de su dueño. "Ellos guardan la información en una base de datos", afirma un especialista.

Isabel Lamoliatte

El 19 de febrero pasado, la policía argentina detuvo en la ciudad de Córdoba a dos hombres y una mujer. Los tres fueron acusados de realizar "varias estafas calificadas de defraudación" durante todo ese mes, según informó el portal transandino "La Voz".

"Colocaban de manera camuflada un dispositivo que debitaba de la cuenta (de la víctima) una X cantidad de dinero", explicó el fiscal cordobés Juan Pablo Klinger. Eran montos pequeños sustraídos, agregó, para "no despertar sospechas".

Pese a la detención del trío de delincuentes, el invento se expandió. A fines de este mes sonaron las alertas en Buenos Aires, cuando un cajero del barrio Palermo, apareció intervenido con un dispositivo similar a la foto.

La importación no tradicional cruzó la cordillera. Aunque el inspector Samuel Inzunza, de la Brigada de Delitos Económicos de la PDI (Bridec), afirma que hasta ahora no han recibido denuncias de víctimas en Chile, ellos están en alerta, debido a que la advertencia de una nueva estafa a través de cajeros automáticos está circulando en redes sociales.

"Está enmarcada dentro del delito de uso fraudulento de tarjetas de crédito y de prepago. También dentro de la Ley 20.009, que limita la responsabilidad de los usuarios en caso de robo, hurto, extravío o fraude de tarjetas bancarias", afirma.

Una disminución

El inspector Inzunza asegura que en el último tiempo la Bridec había detectado una disminución de este tipo de estafa: "La clonación de tarjetas, de manera física a través de cajeros automáticos, se había trasladado a los medios de pago digitales. Habían mutado. Pero con el avance tecnológico las personas que se dedican a estos fraudes se ponen más sofisticadas y crean nuevas fórmulas".

¿Cómo funciona esta fórmula?

"Las estafas van de la mano con las actualizaciones que hacen los bancos de sus sistemas de pago. Los plásticos antes poseían una banda magnética como medida de seguridad. Luego cambiaron a los chips, que se suponían eran más seguros. Algunas ni siquiera traen datos en el plástico para evitar riesgos. No obstante, la tecnología para defraudar al parecer va adelantada y puede leer chips".

¿De qué manera los lee?

"Los dispositivos colocados en el cajero leen los chips. Cumplen una función similar a los POS, la maquinita móvil de Transbank que utilizan en las tiendas y el comercio en general. Cuando una persona inserta su tarjeta en el cajero pasa por encima de este dispositivo fraudulento, que de inmediato lee la información contenida en el chip".

Inzunza detalla que el chip contiene los datos de la tarjeta titular de la cuenta, lo que les permite a los delincuentes acceder a la información, aprovechándose de la tecnología contactless (sin contacto) que la víctima tiene en ese banco.

"El objetivo es captar los números identificatorios del plástico y el dígito de seguridad que aparece detrás de la tarjeta. Cuando tienen estos datos, ellos pueden realizar el fraude después".

¿Ese dispositivo es capaz de leer también la clave que yo creé para mi tarjeta?

"Hasta ahora hemos visto que la información que se extrae de las cuentas de las víctimas debe ser complementada con la clave que cada uno le asigna a su tarjeta de débito. En el caso de las tarjetas de crédito el sistema puede ser más vulnerable, ya que hay tiendas que cuando se paga con esta tarjeta no piden la clave. Basta con acercarla para que se haga el cobro".

> "Cumplen una función similar a los POS, la maquinita móvil de Transbank que utilizan en las tiendas y el comercio en general"
>
> Inspector Samuel Inzunza

El skimmer es capaz de clonar la tarjeta sin necesidad de contacto.

RRSS

El inspector entrega algunas recomendaciones: "Hay que observar bien los cajeros automáticos para detectar si tienen alguna pieza sobrepuesta. Mirar la ranura donde se inserta la tarjeta y el teclado para ver si han sufrido alguna intervención, ya sea que le falte o tenga una pieza de más".

La regla de oro, afirma, sigue siendo cubrir con la mano el teclado antes de ingresar la clave, porque pueden clonar la tarjeta de débito, pero para usarla los ladrones necesitarán una clave. "Al finalizar la transacción, es aconsejable que las personas siempre revisen su cuenta en internet para cotejar que el monto que se giró sea el mismo que aparece en la cuenta".

Similar a los POS

El ingeniero eléctrico y académico de la Facultad Tecnológica de la Usach Gustavo Alcántara, explica que los delincuentes colocan un dispositivo llamado skimmer en el cajero automático: "Este sistema es capaz de leer y capturar los datos desde la banda magnética o del chip. Como usan una tecnología magnética sólo necesitan que la tarjeta se acerque al dispositivo, es similar a lo que hacen los POS en el comercio".

¿De qué manera usan esa información?

"Ellos guardan la información en una base de datos. Los skimmers vienen acompañados de cámaras, que quedan desapercibidas para el usuario, que graban el número de PIN que la persona digita en el teclado. Esos mismos datos son insertados en una nueva tarjeta".

Alcántara aconseja jamás permitir que otra persona manipule nuestra tarjeta. "Hay tiendas donde la máquina parece no leer el plástico. El vendedor ofrece ayuda para acercarla él mismo. Sin embargo, esa maniobra puede ser usada para obtener el código de seguridad que aparece detrás de la tarjeta".