Diálogo Forense
Num. 4, Vol. 2, 2021
ISSN: 2789-8458

Robo de identidad y clonación de tarjetas de crédito y débito utilizando cajeros automáticos alterados

Mayra Alejandra Martínez Ralón
Laboratorio de Informática Forense
Instituto Nacional de Ciencias Forenses de Guatemala –INACIF-
malejandraralon@gmail.com

Recibido: 6/04/2021
Aceptado: 13/10/2021

Palabras clave: Bandeja metálica, cajero automático, clonar, computadora, tarjetas, número de autenticación personal, robo de datos o de identidad, tecnología, teléfono móvil

Key words: Metal tray, ATM, clone, computer, cards, PIN, data breach, technology, mobile phone

RESUMEN

El Laboratorio de Informática Forense del INACIF desde el año 2018 ha recibido múltiples solicitudes del Ministerio Público para realizar análisis relacionados con delitos financieros, bancarios y otros que implican clonación, robo de datos o de identidad personal por medio de tarjetas de crédito y débito; para lo cual se han utilizado cajeros automáticos de distintas entidades del sector bancario, la mayoría de estos casos se suscitan en la ciudad capital de Guatemala.

Los cajeros automáticos o ATM por sus siglas en inglés (Automated Teller Machine) permiten realizar diversas transacciones y trámites utilizando una tarjeta plástica e introduciendo una clave, código o número de autenticación personal PIN (de las siglas en inglés, Personal Identification Number) por medio del teclado del equipo, lo cual permite la autenticación con la entidad bancaria o proveedora del servicio, la mayoría de servicios que brindan estas computadoras implican el uso de dinero (físico o virtual), es por ello que estos equipos se han vuelto sumamente utilizados por la población y, por ende, implicados en muchos casos asociados a estafas.

En Guatemala existen diversas entidades bancarias que ofrecen el servicio a través de cajeros automáticos propios y otras que lo realizan a través de una entidad intermediaria. Muchos de estos equipos han sufrido alguna alteración de parte de criminales para poder obtener los datos impresos en el plástico y número de PIN asociado y con estos poder realizar la clonación o robo de identidad del tarjetahabiente.

En el presente caso de estudio, se analizó el contenido que se generó con el uso de un teléfono móvil, oculto en una bandeja metálica que funcionaba como un sistema de grabación artesanal y que simulaba ser parte del cajero automático, con una pequeña abertura apuntando al lector de tarjetas y al teclado, dicho dispositivo móvil se logró desbloquear en el Laboratorio de Informática Forense y fue posible obtener datos asociados al dispositivo, como los registros cronológicos, y extraer archivos multimedia, como imágenes y videos, en los que se apreciaba el modus operandi de la banda criminal.

ABSTRACT

The Computer Forensic Laboratory of the National Institute of Forensic Sciences (INACIF) has received multiple requests from the Public Ministry since 2018 to carry out analyzes related to financial, banking and other crimes that involve cloning, theft of data or personal identity through credit and debit cards; For which ATMs of different entities of the banking sector have been used, most of these cases arise in the capital city of Guatemala.

Automatic teller machines (ATMs) allow to carry out various transactions and procedures using a plastic card and entering a key, code or personal authentication number (PIN) by the keyboard of the equipment, which allows authentication with the bank or service provider. Most of the services provided by these computers involve the use of money (physical or virtual), which is why these computers have become highly used by the population and, therefore, involved in many cases associated with scams.

In Guatemala there are many banking institutions that offer the service through their own ATMs and others that do it through an intermediary entity. Many of these computers have undergone some alteration by criminals in order to obtain the data printed on the plastic and associated PIN number and with these to clone or steal the identity of the cardholder.

In the present case study, the content that was generated with the use of a mobile phone, hidden in a metal tray that functioned as an artisan recording system and that simulated being part of the ATM was analyzed with a small opening pointing to the reader card and keyboard, it was unlocked in the Forensic Computing Laboratory and it was possible to obtain data associated with the device such as chronological records, extract multimedia files such as images and videos in which the modus operandi of the criminal gang was appreciated.

INTRODUCCIÓN

La falsificación de tarjetas de crédito y débito implica el uso de la tecnología para clonar el plástico o el robo de datos de los titulares de las tarjetas. La metodología que utilizan los delincuentes para realizar el robo de identidad permite que los usuarios no se percaten de las anomalías o fechorías empleadas para robar datos del plástico, muchas veces hurtan únicamente los datos asociados al plástico, sin necesidad de llegar a clonar la tarjeta.

Los cajeros automáticos, o ATM, surgieron en los años 60 (BBC News, 2017) y se han tecnificado y popularizado a través de las décadas debido a la cantidad de servicios que prestan y la facilidad que representa utilizarlos sin necesidad de visitar una agencia bancaria. Actualmente en Guatemala existen miles de estos aparatos, los cuales son manejados por las entidades bancarias o prestadoras de este servicio y gozan de gran aceptación dentro de la población.

Los delitos relacionados con robos por medio de cajeros automáticos se han incrementado debido a la demanda que tienen estos dispositivos, puesto que los delincuentes han utilizado estas cabinas para robar datos de identidad a los usuarios a través de diversas modalidades. Los datos utilizados por los delincuentes son el número de tarjeta, nombres y apellidos, fecha de expiración y número de seguridad (impreso en la parte posterior), los cuales les permiten hacer compras en línea o bien clonarlos a una tarjeta nueva.

Como resultado de estos delitos informáticos, hace su aparición la Informática Forense, como una disciplina auxiliar de la justicia moderna, que utiliza técnicas de adquisición, preservación, obtención y presentación de datos que han sido procesados y almacenados en medios electrónicos y que son aceptados dentro de un proceso legal.

¿CÓMO FUNCIONA UN CAJERO AUTOMÁTICO?

Para el usuario final, el primer paso consiste en introducir una tarjeta plástica en el lector de tarjetas, luego, si se lo pide, marcar el número de PIN en el teclado o la pantalla del cajero automático, posteriormente se ejecuta un proceso de verificación interno que realiza la comprobación de datos con la entidad bancaria y se brinda o se deniega el acceso al tarjetahabiente.

Sin embargo, detrás de estos sencillos pasos existe una estructura electrónica que no es visible para el usuario, que combina tecnología como hardware, software y una red de telecomunicaciones, con estrictos controles de calidad para su correcto funcionamiento.

La Real Academia Española (2021) define el concepto de cajero automático como una "máquina que, accionada por el cliente mediante una clave, realiza algunas funciones propias del cajero encargado de la caja del banco" en la actualidad los usuarios pueden no solamente retirar dinero, sino hacer pagos, consultas y realizar trámites de todo tipo en cuestión de segundos

Los cajeros automáticos suelen ser seguros para su uso ya que las entidades bancarias los utilizan como cajas fuertes y deben velar por brindar a los usuarios cantidades exactas de dinero, a la vez, llevar un minucioso y estricto control de las operaciones y gestiones que se realizan a través de estos. No obstante, algunas bandas criminales manipulan los cajeros para realizar algunos tipos de estafa, por lo que es vital que los usuarios estén atentos y alerta para detectar y reportar cualquier anomalía, previo al uso de los aparatos.

¿CÓMO SE OBTIENEN DATOS PARA FALSIFICAR TARJETAS DE CRÉDITO?

- Los integrantes de la banda criminal fabrican elementos con características similares a las del cajero automático seleccionado para realizar el hurto de datos tomando en cuenta color, materiales y texturas.
- Se coloca un panel falso sobre el original, el cual contiene una pequeña cámara que graba los datos numéricos de las tarjetas colocadas en la abertura para tarjetas y en algunos casos los número de PIN digitados en el teclado.
- La información recolectada es procesada en una computadora y posteriormente se graba en una tarjeta que no ha sido utilizada.
- Luego de falsificar la tarjeta, comienzan a robar dinero a los usuarios.

¿QUÉ ES LA EVIDENCIA DIGITAL?

La evidencia digital es información y datos con valor para una investigación que se almacena, recibe o transmite en un dispositivo electrónico. Esta evidencia se adquiere cuando los datos o los dispositivos electrónicos se confiscan y se guardan para su posterior examen. (National Institute of Justice, 2001)

RESULTADOS DEL PERITAJE INFORMÁTICO FORENSE

Hechos

De acuerdo con los datos obtenidos para la realización del análisis, el indicio objeto de estudio fue recolectado en la ciudad de Guatemala en el último trimestre del año 2017, luego de que la Policía Nacional Civil, la entidad bancaria y el Ministerio Público recibieran varias denuncias de robos a usuarios del cajero automático. El indicio le fue incautado a uno de los delincuentes en flagrancia, mientras lo colocaba en la parte superior de un cajero automático, con el objetivo de copiar información de las tarjetas de débito y crédito de los usuarios para posteriormente clonar las tarjetas y robar dinero (Figura 1).

Según información publicada en varios medios de comunicación, este tipo de delitos lo cometió una banda de clonadores que llevaba meses realizando estas actividades dentro de la ciudad capital y municipios aledaños.

Sobre el Indicio

El indicio consistió en una plancha de metal la cual estaba compuesta por los siguientes elementos (Figura 2):

1. Un teléfono móvil con una tarjeta de memoria para almacenamiento pegada al teléfono
2. Seis imanes redondos
3. Dos baterías externas
4. Cable con conectores USB y micro USB
5. Dispositivo electrónico con conectores USB y micro USB

Objetivos del análisis

Los objetivos planteados para el análisis fueron a) localizar y extraer archivos y registros contenidos en el teléfono móvil y, b) determinar el funcionamiento y la utilización del conjunto de componentes instalados en la plancha de metal.

Sobre la plancha metálica

Se realizó la verificación ocular del indicio y se documentaron todos sus componentes.

La plancha de metal fue localizada en la parte superior del cajero automático, tenía adherido un teléfono móvil, que mediante una pequeña hendidura en la placa metálica alineada con la cámara del dispositivo en mención, era utilizado como sistema de grabación de videos, sonido y de captura de imágenes, apuntando directamente al área de abertura para insertar las tarjetas y del teclado numérico del cajero automático (Figura 3).

El conjunto de componentes

Se documentó el estado del dispositivo y sus características técnicas. El teléfono se encontraba conectado a un módulo de carga elaborado de forma artesanal que constaba de dos baterías externas, un cable y un dispositivo electrónico con conectores micro USB y USB, con el fin de proveer mayor duración de carga al teléfono móvil. Los seis imanes tenían la función de sujetar la plancha metálica a la superficie metálica del cajero.

Obtención de la evidencia digital

El análisis informático forense de dispositivos móviles permite recuperar, extraer, y analizar datos de un dispositivo móvil utilizando diferentes técnicas y herramientas forenses existentes, las cuales se deben de aplicar según el caso. Para llevar a cabo el presente análisis forense se realizó extracción lógica de los datos para el sistema operativo *Android,* lo cual consiste en realizar una copia de los archivos y/o registros almacenados en el teléfono.

El teléfono móvil se recibió bloqueado mediante el método de patrón geométrico de bloqueo y fue desbloqueado manualmente por la perito analista del laboratorio utilizando la técnica denominada *smudge attack*, que consiste en revisar a contra luz las trazas de arrastre que puede dejar el dedo sobre la pantalla del dispositivo.

El mismo tenía instalado el sistema operativo *Android* versión *Marshmallow* y con capacidad de utilizar doble tarjeta SIM, también, contaba con una tarjeta de memoria para almacenamiento externo, la cual no pudo ser extraída del dispositivos para analizarla por separado ya que se encontraba adherida con pegamento al teléfono móvil.

Para realizar la extracción de los datos se colocó el dispositivo en el equipo *Forensic Recovery of Evidence Devices* (FRED) y se seleccionó el método de extracción *Logical Android Backup* que brinda la herramienta *forense Cellebrite UFED Touch*, la cual permite realizar la extracción de datos de los dispositivos móviles.

Finalmente se cargaron los datos en el equipo *Forensic Recovery of Evidence Devices* (FRED) y se procesó el archivo de la extracción con el UFED *Physical Analyzer*, que es un programa forense de análisis, decodificación de datos y de generación de informes que permite visualizar el contenido de las extracciones para poder analizar los datos obtenidos y mostrarlos mediante un informe que puede ser emitido en formato HTML (es un lenguaje que se utiliza para el desarrollo de páginas de Internet), pdf, Microsoft Excel o formato propietario UFED Reader.

Mediante lo anterior, se lograron recuperar y extraer los siguientes datos digitales:

- Datos físicos y lógicos de identificación del dispositivo para realizar la comparación del IMEI *(International Mobile Station Equipment Identity en inglés)* que es un código regularmente de 15 dígitos impresos de forma física detrás de la batería del teléfono y de forma lógica marcando el código *#06#; datos que permiten identificar inequívocamente al equipo móvil.

- Videos con fecha y hora de grabación que documentan las grabaciones de los números impresos en el plástico y códigos o PINES ingresados por los usuarios.

- Aplicaciones móviles instaladas.

- Archivos de imagen con metadatos que registran ubicación, fecha y hora de captura, entre otros datos.

- Cronograma de eventos, una línea de tiempo gráfica que permite estructurar el historial de los eventos y revisar un lapso de tiempo en específico.

A todo el material obtenido le fue generado su propio valor *hash,* lo que permite asegurar que la extracción decodificada es la misma que la que se recibió del dispositivo originalmenteLas bandas criminales de clonadores utilizan técnicas inusuales y sofisticadas para la clonación y robo de identidad, a través de las tarjetas de crédito y débito, muchas de esas acciones son desapercibidas por los usuarios de los cajeros automáticos o ATM.

CONCLUSIONES

Las bandas criminales de clonadores utilizan técnicas inusuales y sofisticadas para la clonación y robo de identidad, a través de las tarjetas de crédito y débito, muchas de esas acciones son desapercibidas por los usuarios de los cajeros automáticos o ATM.

Este caso de estudio, deja en evidencia la forma transparente en que fue colocado el objeto metálico, el cual tenía adherido un teléfono móvil, contaba con un método externo de carga y era utilizado como sistema de grabación de videos, sonido y de captura de imágenes.

El dispositivo móvil con sistema operativo *Android*, fue desbloqueado en el laboratorio de informática forense, se le extrajeron datos empleando los métodos para análisis forense de dispositivos móviles y análisis forense de medios de almacenamiento digital y otros dispositivos, se utilizaron las herramientas *forenses Cellebrite UFED Touch* y *Cellebrite Physical Analyzer* y, posterior al análisis de las extracciones y los componentes del dispositivo metálico que era utilizado como dispositivo de grabación, se entregaron a la fiscalía documentos en los cuales se reportaron líneas de tiempos que permitieron monitorear eventos mediante una vista cronológica, archivos multimedia de videos (de larga duración) e imágenes que documentan la forma en que se grababa a los usuarios de las tarjetas digitando los pines para utilizarlas y documentando el número y nombre impreso en la parte superior del plástico. Asimismo, estos archivos permitieron observar las pruebas que realizaron los delincuentes previo a dejar instalado el artefacto metálico en el cajero automático.

En la actualidad, la informática y sus ramas tienen un crecimiento exponencial que nos enfrenta a grandes retos en todos los ámbitos, debido a la diversificación y masificación de las tecnologías de la información y la comunicación (TIC´s).

Derivado de lo anterior, el laboratorio de informática forense ha desarrollado una metodología de trabajo basada en el conocimiento, experiencia y pericia adquirida por el capital humano que lo conforma, quienes se encargan de realizar la investigación y desarrollo de los procesos para los distintos tipos de análisis que se llevan a cabo; implementando la mejora continua, mediante la revisión y control constante de los procesos internos y de gestión de la calidad.

RECOMENDACIONES

Para detectar y evitar ser víctimas de fraudes mediante cajeros automáticos, se recomienda tomar en consideración los siguientes aspectos:

- Revisar la estructura del cajero, muchos de los elementos alterados están pintados o revestidos del mismo color y contienen cámaras y otros artefactos que pueden grabar la clave o PIN y otros datos útiles asociados a la cuenta.
- Verificar si hay objetos flojos en el teclado o en la abertura para insertar la tarjeta, que hayan sido adheridos falsamente.
- Revisar la ranura en donde se inserta la tarjeta, observar algún artefacto extraño o que engrose la ranura. Existen dispositivos llamados skimmers que pueden copiar los datos y clonar la tarjeta.
- Utilizar cajeros automáticos ubicados en sitios seguros, iluminados y observar si existen cámaras de grabación cercanas.
- No utilizar un cajero automático si existe sospecha que ha sido alterado, e informar a la entidad bancaria de manera oportuna.
- Observar previo a utilizar el cajero automático si hay individuos sospechosos.
- Cambiar el PIN periódicamente.

BIBLIOGRAFÍA

BBC News. (27 de Junio de 2017). Recuperado el 24 de Febrero de 2021, de https://www.bbc.com/mundo/noticias-40417156

Cellebrite. (2013-2014). Cellebrite Certified Logical Operator. Cellebrite USA Inc.

Cellebrite. (s.f.). *Cellebrite Productos.* Recuperado el 1 de Marzo de 2021, de Díaz González, C. R., Hernández Arroyo, J. E., & Ríos Ruiz, V. (Abril de 2016). Forensic Analysis of Computers and Other Electronic Devices. (ICF-1092-LAB), 14. San Juan, Puerto Rico: Institute of Forensic Sciences.

EL PAÍS . (14 de Febrero de 2007). *El País*: *Diario* . Recuperado el 3 de Marzo de 2021, de https://elpais.com/diario/2007/ 02/15/madrid/1171542258_740215.html

El Periódico. (26 de Septiembre de 2017). *El Periodico:* Nacionales. Recuperado el 26 de Febrero de 2021, de https://elperiodico.com.gt/nacionales/2017/09/26/buscan-desarticular-banda-de-clonadores-de-tarjetas/

LA TERCERA. (18 de Julio de 2019). Detectan dispositivos para clonar tarjetas en el Banco Francés de Adrogué. *DIARIO LA TERCERA.*

Martínez, A. (23 de Febrero de 2016). *INCIBE-CERT.* Recuperado el 13 de Septiembre de 2021, de https://www.incibe-cert.es /blog/herramientas-forense-moviles

National Institute of Justice. (2001). *National Institute of Justice*. Obtenido de https://www.ojp.gov/pdffiles1/nij/219941.pdf

Newman, R. C. (2007). *Computer Forensics: evidence, collection, and management* (Primera ed.). Boca Raton: Auerbach Publications.

Prensa Libre. (s.f.). *Prensa Libre:* Justicia. Recuperado el 26 de Febrero de 2021, de https://www.prensalibre.com /guatemala/justicia/detienen-a-clonador-de-tarjetas-cuando-instalaba-dispositivos-en-cajeros/

Prensa Libre. (s.f.). *Prensa Libre:* Justicia. Recuperado el 24 de Febrero de 2021, de https://www.prensalibre.com/ guatemala/justicia/capturan-a-clonadores-de-tarjetas-de-credito-y-debito-guatemala/

Real Academia Española. (s.f.). *Diccionario de la lengua española.* Recuperado el 1 de Marzo de 2021, de https://dle.rae.es/cajero

Superintendencia de Bancos. (s.f.). *Superintendencia de Bancos*: alerta al público. Recuperado el 5 de Marzo de 2021, de https://www.sib.gob.gt/web/sib/alerta_al_publico

FIGURAS

Figura 1- Imagen con fines ilustrativos-obtenida de internet Fuente: https://www.diariolatercera.com.ar/nota/35631-detectan-dispositivos-para-clonar-tarjetas-en-el-banco-frances-de-adrogue/

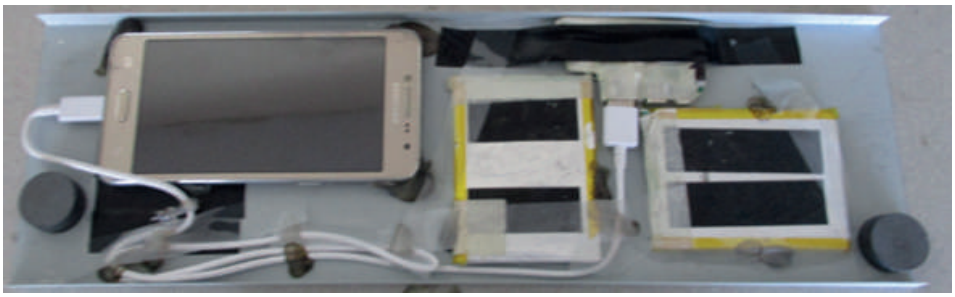

Figura 2 – Plancha metálica

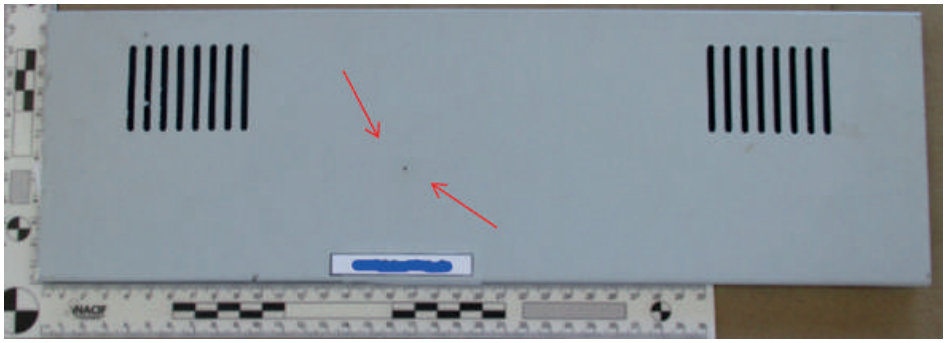

Figura 3 – Abertura para cámara de grabación

Figura 4 – Grabación real del cajero automático

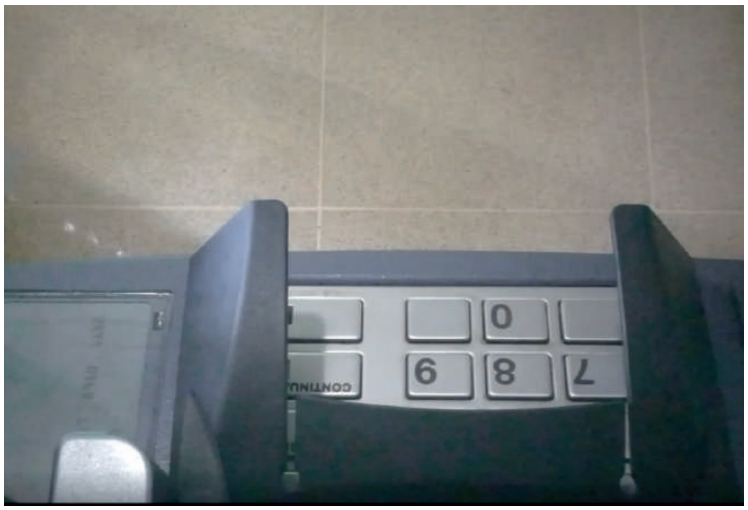

Figura 5 – Grabación real del cajero automático

Figura 6 – Grabación real del cajero automático

Figura 7 – Grabación real del cajero automático

Figura 8 – Grabación real del cajero automático