EDP UNIVERSITY

RECINTO DE HATO REY

PROGRAMA DE MAESTRIA EN SISTEMAS DE INFORMACION

CON ESPECIALIDAD EN SEGURIDAD DE INFORMACION DE FRAUDE DIGITAL

FRAUDE ELECTRONICO A UN CAJERO AUTOMATICO (ATM)

ANALISIS DE CASO: United States v Chris Suhail Folad / Khaled Nabil Abdel Fattah

Caso Núm.: 3:14-cr-00168

DICIEMBRE, 2019

PREPARADO POR

JESSICA BÁEZ SÁNCHEZ

Sirva la presente para certificar que el Proyecto de Investigación titulado:

FRAUDE ELECTRONICO A UN CAJERO AUTOMATICO (ATM)

ANALISIS DE CASO: United States v Chris Suhail Folad / Khaled Nabil Abdel Fattah

Caso Núm.: 3:14-cr-00168

Preparado por

Jessica Báez Sánchez

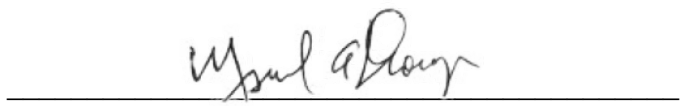
Ha sido aceptado como requisito parcial para el grado de

Maestría En Sistemas De Información

Con Especialidad En Seguridad De Información E Investigación De Fraude Digital

Diciembre, 2019

Aprobado por:



Prof. Miguel A. Drouyn Marrero

DEDICATORIA

Dedico este proyecto primero a DIOS, por darme las fuerzas, ánimos y garras para realizar este curso culminando con buenas notas y con bastante conocimiento en esta maestría el cual me permitirá prosperar económica y profesionalmente

A mi hijo Gabriel, que es un milagro en mi vida, y mi razón de ser, comencé mis estudios con el embarazo y no me retire de los estudios al contrario continúe para luchar por él y para él.

A mi padrastro Juan Torres que me ayudo con su apoyo incondicional, para que estudiara y progresara en la vida, creyó en mí y en mi potencial para estudiar en un curso que será beneficioso en mi vida profesional y económicamente.

A mi madre Carmen Sánchez, por apoyarme para completar mis estudios, y tener un mejor trabajo.

A mi esposo Juan Carlos Lleras, que sin su ayuda y comprensión conmigo y con mi hijo no hubiera podido hacer realidad mis estudios

Para ellos es esta dedicatoria de este análisis de proyecto, pues es a ellos a quienes se las debo por su apoyo incondicional.

TABLA DE CONTENIDO

INTRODUCCIÓN Y TRASFONDO

Introducción

En este caso se presentan dos individuos que fueron acusados por robo mediante uso de contraseñas y codificación de tarjetas para retiro de dinero en las maquinas ATM. Como parte de la investigación se demuestra que los acusados robaron por un tiempo prolongado una cantidad de dinero sin que la compañía dueña de las maquinas ATM, se dieran cuenta hasta que se realizó una auditoría interna.

Según se desprende en los documentos judiciales se informa que estos dos individuos utilizaron contraseñas y "master code" para acceder a los compartimientos o "cassette" de la ATM para robar. Los "cassette" son los compartimientos donde se guarda el dinero de la caja registradora. Estas cajas registradoras que dependían del tamaño y programación de su sistema podrían guardar hasta siete compartimientos. La empresa afectada es nombrada como Safe Cash Systems, LLC. con sede en Nashville, coloca máquinas en tiendas de conveniencia, bares y restaurantes en todo Nashville.

Khaled Nabil Abdel Fattah (acusado)

Cajero Automático (ATM) Modelo C4000

Descripción del Caso

Nombre del Caso: USA vs Chris Suhail Folad and Khaled Nabil Abdel Fattah

Número del Caso: 3:14CR00168

Partes del Caso

Acusado (s)

Chris Suhail Folad

Khaled Nabil Abdel Fattah

Victimas u otras personas o entidades involucradas

Safe Cash Systems, LLC

Investigadores

Abogados Defensa

Cynthia Sherwood – Abogado de Defensa Chris Suhail Folad

Bob Peal – Abogado de Defensa Khaled Nabil Abdel Fattah,

William T. Ramsey – Abogado de Defensa Khaled Nabil Abdel Fattah

Abogados – Gobierno

Henry Leventis – Abogado del Gobierno

Fiscal

Hilliard Hester - Assistant United States Attorney, USDC Tennessee

Juez de Distrito

Aleta Arthur Trauger - United States District Judge of the United States District Court for the Middle District of Tennessee

Trasfondo

El fraude cometido por estos dos individuos Folad y Fattah fue realizado desde 22 de octubre de 2009 hasta 4 de marzo de 2010 en Tennessee en la cual uno de los acusados trabajaba en esa empresa como técnico reparador de las maquinas ATM. Los cargos presentador por la compañía afectada ante el tribunal fue en el octubre 2014 y fue a juicio en 16 de mayo de 2016 **(USA vs Chris Suhail Folad and Khaled Nabil Abdel Fattah, Transcript of proceedings, 16 de mayo de 2016).**

Según el documento presentado al tribunal **(USA vs Chris Suhail Folad and Khaled Nabil Abdel Fattah Indicment, 22 de octubre de 2014)** La denuncia inicial comenzó por un defalco en las maquinas ATM, en el cual utilizaba las contraseñas de las maquinas ATM que mientras se le estaba dando mantenimiento a los cajeros automáticos, y programó las mismas para expedir billetes de $20 en vez de billetes de $1 cuando se realizaban pruebas técnicas.

El ex técnico utilizó sus conocimientos en reparación y mantenimiento de las maquinas ATM y realizó en varias de las maquinas que él le dio servicio, un defalco de miles de dólares sacando billetes de $20 en vez de billetes de $1.

La compañía Safe Cash una vez notaron los desfalcos de varias máquinas ATM y comenzaron una investigación hasta dar con el resultado que estos fraudes provenían de la misma persona un ex técnico de la compañía el cual tuvo acceso al sistema del cajero automático. Como el defalco de dinero supera la cantidad de $200,000 entra en la investigación

el servicio secreto, por tanto, realizaron auditorias y búsqueda en las maquinas ATM, pero estas no presentaban toda la evidencia ya que se borraba la información después de varias transacciones.

Descripción de los hechos

Según el documento judicial **(USA vs Chris Suhail Folad and Khaled Nabil Abdel Fattah Indicment, 22 de octubre de 2014)** El fraude cometido por estos dos individuos Folad y Fattah fue realizado desde enero 2009 hasta marzo 2010. Folad y Fattah utilizaron contraseñas para los cajeros automáticos de una empresa local para alterar las cantidades de distribución de la denominación para llevar a las máquinas a creer que estaban dispensando billetes de $1, cuando, de hecho, las máquinas dispensaban billetes de $20. El acusado Folad anteriormente trabajó en Safe Cash como técnico de cajeros automáticos y conocía las contraseñas necesarias para cambiar las cantidades de distribución de denominación.

Los acusados fueron condenados por un jurado federal, después de un juicio de tres días, de conspiración por cometer fraude de acceso informático y fraude en línea de transferencia bancaria, los cargos aplicados fueron 19 cargos individuales de fraude de acceso informático y 11 cargos de fraude en línea de transferencia bancaria. La investigación fue realizada por el Servicio Secreto de Estados Unidos.

Acusaciones, cargos y penalidades

(USA vs Chris Suhail Folad and Khaled Nabil Abdel Fattah Indicment, 22 de octubre de 2014)

Conspiración cometer fraude electrónico - 18 U.S.C. § 371

Fraude de acceso a la computadora -18 U.S.C. § 1030 (a) (4)

Fraude electrónico - 18 U.S.C. § 1343

Decomiso criminal -18 U.S.C. § 982 (a) (2) (B)

Definición de términos

ATM Journal: reporte diario de las transacciones de la maquina ATM

Worldpay: programa que está instalado en la maquina ATM, para contar y transmitir la información de dinero.

Morphis: es un programa que genera el promedio de uso diario durante el mes y genera un informe para saber cuándo deben recargar la maquina con efectivo.

REVISIÓN DE LITERATURA

Introducción

Existen varios tipos de fraude y riesgos utilizando dispositivos como computadoras o equivalentes, en este caso fue mediante un cajero automático o ATM. Los autores de este caso lo son Chris Suhail Folad y Khaled Nabil Abdel Fattah, estos fueron condenados por un jurado federal, después de un juicio de tres días, por un cargo de conspiración por cometer fraude de acceso informático y fraude de transferencia electrónica, 19 cargos individuales de fraude de acceso informático y 11 cargos de fraude electrónico (wire fraud). La confianza de estas personas llevó a tal nivel que por el fraude cometido han sido sentenciados a 20 años de cárcel. Los primeros $20 salieron que retiraron fue de una de sus propias cuentas bancarias, esto para probar el sistema y así poder conocer que el fraude podría ser cometido y seguir utilizando este formato para sacar más dinero. Los acusados al principio estaban usando sus propias tarjetas de cuenta de banco. Pero luego de la primera transacción, utilizaron el dinero que contenía los compartimientos dentro del cajero automático.

Safe Cash ordenó a sus empleados y técnicos de los cajeros automáticos, que verificaran los registros de uso de cada una de las ATM que tenían en diferentes localidades para verificar si había algo fuera de sus registros o si las ATM estaban funcionando correctamente, ya que tenían sospecha de unos registros que no concordaban y además estaban rellenando las ATM más veces de las que normalmente se rellenaban. Debido a que los cajeros automáticos almacenan un número limitado de transacciones, los empleados no pudieron encontrar entradas de registro para muchos de los retiros sospechosos. Durante su investigación localizaron algunas de las entradas de registro de cuatro de los cajeros, e imprimieron algunos de esos registros y la proporcionaron a los funcionarios federales encargados de hacer cumplir la ley en 2010.

Luego de que se realizara la investigación y el esquema había sido encontrado, el dueño de Safe Cash se le solicito reemplazara la totalidad de sus cajeros automáticos ya que no cumplían con las leyes federales, además que tenían una vulnerabilidad activa en su programación que esta permitió el acceso no autorizado al sistema del cajero automático. Permitiendo que el ex técnico Khaled Nabil Abdel Fattah manipulara el sistema e ingresar a los compartimientos dentro del cajero automático y este despachara dinero cambiando sus denominaciones.

El propietario de los cajeros automáticos había determinado lo que había sucedido, y reemplazaron diecisiete de los dieciocho cajeros automáticos ya que solo uno de los cajeros automáticos cumplía con las leyes federales el cual exige que las ATM sean accesibles para las personas con deficiencias de la vista. Estos cambios de los cajeros automáticos provoco según los acusados la destrucción de pruebas potencialmente exculpatorias. Por esta razón los acusados continúan solicitando que se les baje la sentencia ya q la empresa cambió los cajeros automáticos y no existe pruebas acusatorias.

Fraudes involucrados

Según algunos artículos encontrados en una reciente búsqueda de información **(los fraudes más comunes en los cajeros automáticos y como evitarlos, 3 de octubre de 2018)** nos informa que la ley federal define al fraude electrónico como el uso de una computadora con el objetivo de distorsionar datos para inducir a otra persona a que haga o deje de hacer algo que ocasiona una pérdida. Los delincuentes pueden distorsionar los datos de diferentes maneras.

Primero, pueden alterar sin autorización los datos ingresados en la computadora. Un individuo puede usar fácilmente este método para alterar esta información y malversar fondos de una empresa. En segundo lugar, los delincuentes pueden alterar o borrar información

almacenada. Tercero, los delincuentes sofisticados pueden reescribir los códigos de software y cargarlos en la computadora central de un banco para que éste les suministre las identidades de los usuarios. Los estafadores luego pueden usar esta información para realizar compras no autorizadas con tarjetas de crédito.

Otro tipo de esquemas encontrado en fraude electrónico a los cajeros automáticos son los "ATM jackpotting", (**ATM 'Jackpotting' Attacks Reveal Deeper Problems, Feb 12, 2018)** el cual consiste en la explotación de vulnerabilidades físicas y de software en máquinas bancarias automatizadas que dan lugar a que las máquinas dispensan dinero en efectivo. Con acceso físico a una máquina, el "ATM jackpotting" permite el robo de las reservas de efectivo de la máquina, que no están vinculadas al saldo de ninguna cuenta bancaria. Los ladrones que tienen éxito y permanecen sin ser detectados pueden irse con todo el dinero de la máquina.

Los culpables utilizan una computadora portátil para conectarse físicamente al cajero automático y utilizar un malware. ATM Jackpotting. " usando una secuencia de botones especial y algunos conocimientos internos, es posible reconfigurar los cajeros automáticos para creer que están dispensando billetes de un dólar, en lugar de veinte dólares. Por otro lado, se encuentra el fraude Tyupkin, en estos años aumentó el fraude hacia los cajeros automáticos y otros fraudes bancarios. Cada vez se aumenta los tipos de fraude ya que los delincuentes continúan en la búsqueda para crear otros conceptos para cometer fraude.

El fraude Tyupkin, según encontramos durante la búsqueda de fraudes electrónicos (**Tyupkin: Un programa malicioso que manipula cajeros automáticos (octubre 7, 2014)** define este concepto como un tipo de malware que permite a los cibercriminales vaciar el dinero de cajeros automáticos mediante manipulación directa. Este malware, detectado por Kaspersky Lab como Backdoor.MSIL.Tyupkin, afecta a cajeros automáticos de los principales fabricantes

de cajeros automáticos que ejecutan Microsoft Windows de 32 bits. Basada en esta información encontrada podemos definir que el concepto "tyupkin" fue el fraude que utilizaron los acusados de este caso, para la fecha que fue realizado el fraude este concepto no había sido definido, no fue hasta que ocurrió este caso que se presentó esta definición.

Leyes aplicables

18 U.S.C. § 371 Conspiración para defraudar los Estados Unidos o cualquier otra agencia, esto significa que dos o más personas conspiran para cometer cualquier delito contra los Estados Unidos u otra agencia de cualquier manera como fraude electrónico y fraude de acceso a la computadora para un propósito. Esta ley no sólo alcanza la pérdida financiera o de propiedad a través del uso de un esquema o artificio para defraudar, sino que también está diseñada y destinada a proteger la integridad de los Estados Unidos y sus agencias, programas y políticas.

18 U.S.C. § 1030 (a) (4) Fraude y actividad relacionada en relación con computadoras este significa realizar un fraude a sabiendas y con la intención de defraudar utilizando acceso a la computadora protegida sin autorización, lo que ha provocado daños especificados como pérdida monetaria de por lo menos $5,000 y para el tráfico de una contraseña o información similar.

18 U.S.C. § 1343 Fraude electrónico, radio o televisión, esta ley representa persona con intención o idear cualquier esquema de fraude para obtener dinero o propiedad por medio de fraude electrónico, falsas representaciones, utilizando cable o transferencia electrónica, con el fin de ejecutar dicho esquema, será multado bajo este título o encarcelado no más de 20 años, o ambos.

18 U.S.C. § 982 (a) (2) (B), que tras la condena de la conspiración y el acceso a la computadora. El tribunal, al imponer sentencia a una persona condenada por un delito en

violación, ordenará que la persona pierda a los Estados Unidos cualquier propiedad, real o personal, involucrada en dicho delito.

Casos relacionados

USA vs Ercan Findikoglu (2013) United Statesv Ercan Findikoglu Indictment (25 de julio de 2013)

> Tan reciente como en marzo, el "hacker" turco Ercan Findikoglu, conocido en internet como "Segate" o "Predator", se declaró culpable de robar $55 millones USD de cajeros automáticos de Nueva York y del mundo. El estafador, logró eludir una búsqueda internacional durante cuatro años, se enfrenta a hasta 14 años de prisión como parte de un acuerdo con los fiscales. En 2013, Findikoglu realizó 36,000 operaciones en 24 países consiguiendo 40 millones de dólares, según las autoridades.
>
> En noviembre del año pasado, más de 50 personas reportaron fraudes en cajeros automáticos. La cifra representó un incremento del 46% en comparación con el mismo periodo para 2014. Las estafas ocurrieron principalmente en establecimientos de la cadena 7-Eleven.

USA v Zhang Qiaocheng (2018) USA v Zhang Qiaocheng and Zhang Xioalang Criminal Complaint (9 de julio de 2018)

> Los acusados Zhang Qiaocheng y Zhong Shaowen fueron presuntamente detectados en condiciones sospechosas alrededor de un cajero automático instalado en una sucursal de HBL en Abdullah Haroon Road durante dos días.

El 10 de enero de 2018, los funcionarios de la FIA los capturaron a las 8:15 pm mientras intentaban insertar un dispositivo de desnatado en dicho cajero automático al comprometer el acceso no autorizado al sistema de información de infraestructura crítica con la intención de causar daños a la propiedad pública.

Herramientas de investigación

Para la investigación de este tipo de fraude fue realizado mediante una auditoría interna, además se utilizó el programa de FTK Forensic Toolkit para establecer y detectar las irregularidades del sistema y de las transacciones que realizaron durante un tiempo específico. Los cajeros automáticos tienen un programa que solo guarda una cierta cantidad de transacciones lo cual se les hace imposible realizar la auditoria y llegar a las transacciones donde estuvo el descuadre o la alteración del cajero automático. El programa FTK Forensic Toolkit es un programa que puede detectar data eliminada de nuestra base del equipo electrónico que estemos en proceso de investigar. Este equipo es regulado por una institución privada y no por el gobierno por tanto ellos no tienen regulación de las transacciones.

La herramienta de FTK Forensic Toolkit es considerada un estándar de excelencia en la industria de la investigación forense y es altamente aceptada en procesos investigativos conducidos por el FBI, Interpol y múltiples agencias de ley y orden. Esto garantiza que el proceso investigativo realizado por cualquier investigador forense cumple o excede los requisitos establecidos por el Gobierno Federal para el procesamiento, preparación y entrega de evidencia a ser utilizada en proceso judicial.

SIMULACIÓN

Introducción

Según el documento jurídico, **USA vs Chris Suhail Folad and Khaled Nabil Abdel Fattah, Transcript of proceedings (mayo, 16, 2016).** el caso comenzó a ser investigado en el 2014, cuando notaron una irregularidad en las transacciones realizadas en varias máquinas ATM que eran propiedad de la compañía Safe Cash. Estas máquinas ATM estaban localizadas en Nashville, Tennessee, según ronda la investigación una vez la compañía sospecha que existe una irregularidad en algunas transacciones realizadas durante los años 2009 y 2010. La compañía Safe Cash solicita a uno de sus técnicos de la ATM realice una investigación o una auditoría interna sobre las transacciones para verificar si existe o existió alguna irregularidad en sus cuentas, ya que encuentran una disparidad en la numeración de las transacciones. Estos revisan sus equipos y programas en el cual encuentran una incongruencia de números en los récords.

Estos técnicos deben tener numeraciones de sus informes antes de recargar la máquina y después de recargar la misma. Estas numeraciones deben estar acorde con sus informes tanto en el programa que utiliza la ATM como en la empresa, estos los programas les provee información de la fecha, cantidad y transacciones que se realizan en cada cajero automático, uno de los programas utilizados es el Worldpay. Una vez la compañía nota la irregularidad, la investigación es escalada hacia el Servicio Secreto de Estados Unidos ya que el fraude financiero que supere los $200,000 es responsabilidad del Servicio Secreto entrar a realizar una investigación.

TEORIA DEL ESQUEMA DE FRAUDE

Khaled Fattah and Chris Folad

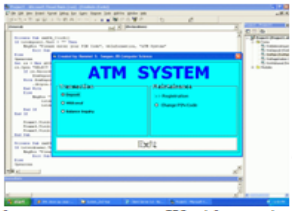
SafeCash ATM
Modelos 1500, 2100, c4000

Pantalla de la ATM, mediante se realizaba los cambios de transacciones por el técnico

Cada modelo de ATM tiene su control interno que son los master code para realizar cambios en sus sistemas

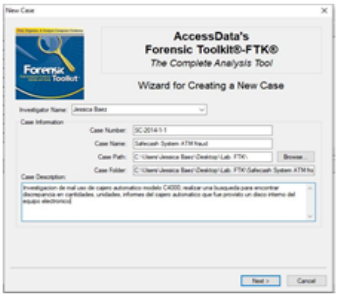
Luego de ingresar el código, cambiaban la cantidad a dispensar billetes de $20 en vez de billetes de $1, hicieron un centenar de transacciones

Luego de realizar varias transacciones, la compañía se dio cuenta del fraude y comienza una investigación y auditoria interna



Utilizando programa como Worldpay, el cual indica las transacciones, números, fechas, horas, codificación, encontraron el fraude, ahora falta revisar quien realizo el mismo.

Entra en investigación el Servicio Secreto de EEUU



Para poder acceder al Sistema, utilizaron varios programas entre ellos Kali, y FTK Forensic Toolkit estos accedieron al Sistema encontrando los archivos y transacciones. Encontrando incongruencias en las numeraciones donde brincaban las numeraciones de las transacciones que Worldpay mostraba en sus sistemas.

INFORME FORENSE DEL CASO

Resumen Ejecutivo

Esta investigación es relacionada al caso contra Chris Suhail Folad y Khaled Nabil Abdel Fattah por defalco a la empresa SafeCash, Systems LLC, compañía dedicada a la distribución, venta de piezas y servicio al cliente de máquinas ATM, en negocios, hoteles, bares, entre otros. Esta empresa cuenta con más de 200 máquinas ATM distribuidas en diferentes ciudades del estado de Tennessee, Cada ciudad cuenta con varios técnicos para el arreglo y depósitos de efectivo, retiro de efectivo de los cajeros automáticos. El Sr. Eric Rivera quien es el fiscal del caso, solicita los servicios de la investigadora forense Jessica Baez de JBS Internet Security Group para investigar un cajero automático, en el cual se había encontrado una discrepancia es sus cantidades que se depositaban vs la cantidad que mantenía este cajero automático ATM.

Por tal razón el Sr. Eric Rivera le entrega a la investigadora forense Jessica Báez de JBS Internet Security Group un dispositivo USB el cual contiene una imagen la información del disco duro interno de la ATM para ser investigador y verificar evidencia sobre alguna discrepancia en la numeración o en el registro del equipo.

Según el fiscal Rivera el disco interno a investigar forma parte del cuerpo de evidencia recolectado por los agentes del Servicio Secreto en los allanamientos efectuados a la maquina ATM modelo C4000.

Objetivos

Exponer las evidencias encontradas en la investigación realizada al equipo electrónico incautado mediante el análisis de la imagen del disco duro de la máquina del cajero automático y realizar un informe detallado de la investigación. Exponer además las transacciones de retiro de dinero que fueron realizadas por los acusados usando los siguientes programas y equipos de

investigación forenses que se encuentran en nuestras oficinas. El programa que utilizó durante esta investigación será el programa de FTK Forensic Toolkit.

Alcance del trabajo

- Se realizó la investigación usando el programa FTK Forensic Toolkit, esta herramienta es considerada uno de los estándares de excelencia en la industria de la investigación forense y son altamente aceptadas en procesos investigativos conducidos por el FBI, Interpol y múltiples agencias de ley y orden. Esto garantiza que el proceso investigativo realizado por JBS Internet Security Group cumple o excede los requisitos establecidos por el Gobierno Federal para el procesamiento, preparación y entrega de evidencia a ser utilizada en proceso judicial. Se investigó las transacciones realizadas en el cajero automático durante el periodo 2009 al 2010.

Datos del caso

- **Número del Caso:** SC-2014-1-1
- **Investigador:** Jessica Báez Sánchez
- **Cliente solicitante de la Investigación:** SafeCash Systems, LLC
- **Representante de la empresa:** Juan Lleras

Descripción de los dispositivos utilizados

Se investigó el dispositivo electrónico USB que contiene la imagen del disco duro de la ATM modelo C4000. Este USB será evaluado en el equipo forense de nuestras oficinas, utilizando el programa de FTK Forensic Toolkit, Se creará una copia original fiel y exacta en nuestros archivos para mantener el dispositivo original y este no sea dañado.

Resumen de los hallazgos

El proceso de análisis forense digital envuelve la adquisición, preservación, análisis, y presentación de evidencia digital. Este tipo de evidencia es frágil y el investigador podría, sin darse cuenta alterar, o destruir la información contenida en algún dispositivo que está siendo objeto de análisis. Esto trae como consecuencia que esta evidencia sea declarada inadmisible ante un tribunal.

En la prueba se pudo demostrar que después de que las cantidades de la distribución de la denominación fueran cambiadas, los demandados recibirían 20 veces más efectivo de las máquinas que el monto que fue cargado de sus cuentas bancarias. Durante un período de 14 meses los acusados realizaron más de 800 retiros de cajeros automáticos dinero en efectivo, haciendo hasta 20 retiros de cajeros automáticos en un solo día. Los acusados utilizaron nueve cuentas bancarias y 17 tarjetas bancarias para perpetrar su fraude y robaron más de $600.000.

Figura 1 – Formato en programa sobre registro de usuarios y pin number

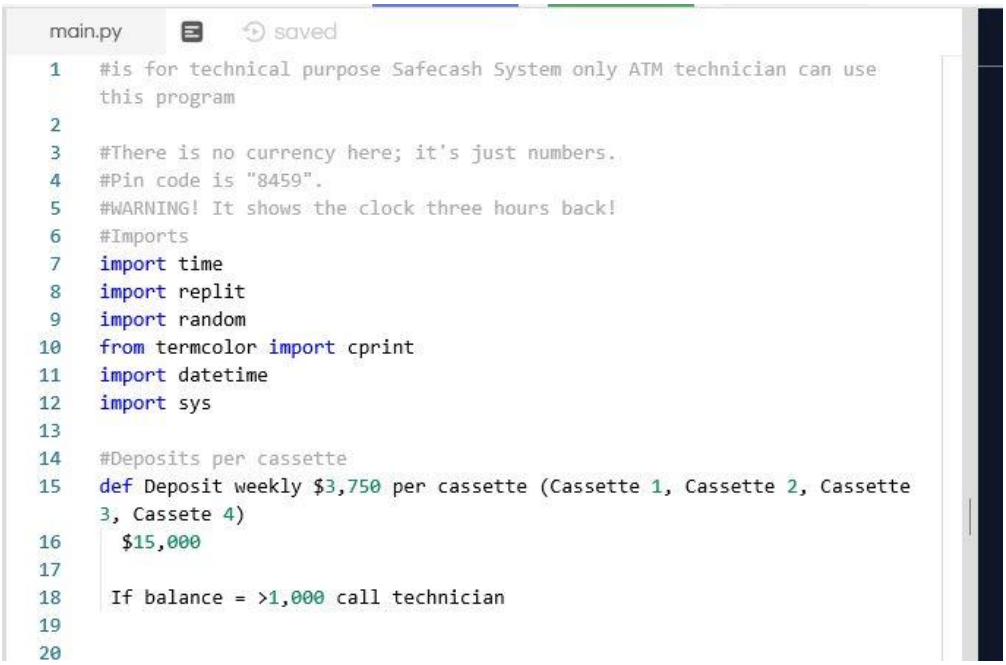
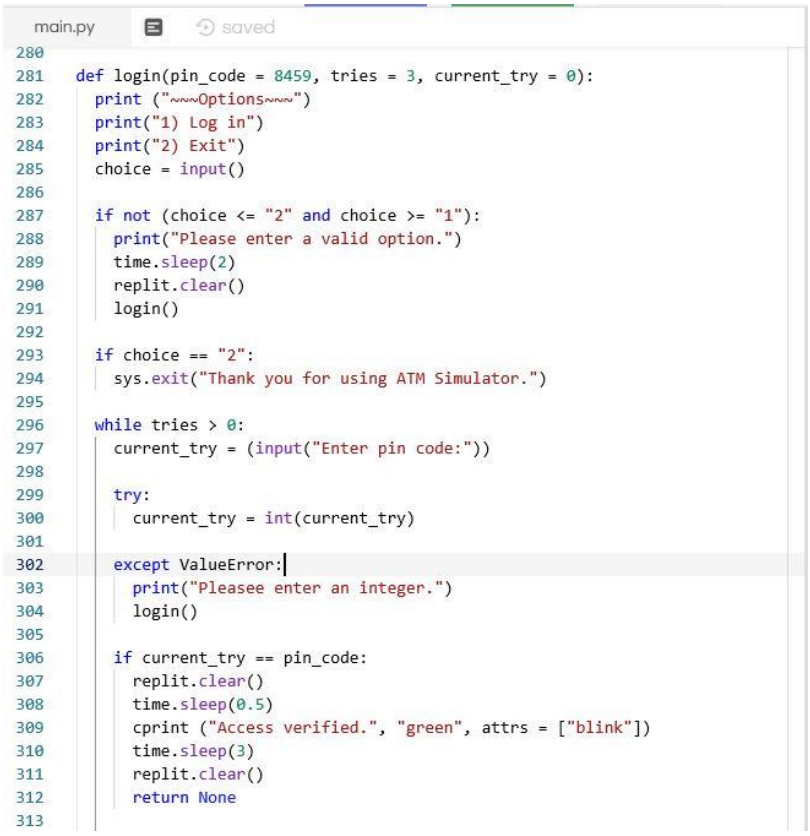


Figura 2 – Formato para entrada de registro de usuarios por medio de pin, con programación para entrada del usuario y su aprobación



```
main.py   saved
280
281  def login(pin_code = 8459, tries = 3, current_try = 0):
282    print ("~~~Options~~~")
283    print("1) Log in")
284    print("2) Exit")
285    choice = input()
286
287    if not (choice <= "2" and choice >= "1"):
288      print("Please enter a valid option.")
289      time.sleep(2)
290      replit.clear()
291      login()
292
293    if choice == "2":
294      sys.exit("Thank you for using ATM Simulator.")
295
296    while tries > 0:
297      current_try = (input("Enter pin code:"))
298
299      try:
300        current_try = int(current_try)
301
302      except ValueError:
303        print("Pleasee enter an integer.")
304        login()
305
306      if current_try == pin_code:
307        replit.clear()
308        time.sleep(0.5)
309        cprint ("Access verified.", "green", attrs = ["blink"])
310        time.sleep(3)
311        replit.clear()
312        return None
313
```

Figura 3 – Programación de los compartimientos o “cassette” para entrada de información

```
422
423       <!-- CASSETTES -->
424       <div id="hardware-page" hidden="true">
425         Under construction
426         <div class="row" id="cassettes-row">
427           <div class="col-xs-3 cassette-area">
428             <div class="row">
429               Cassette 1
430               <form id="cassette-1-form" class="navbar-form navbar-left" title="">
431                 <div class="row">
432                   <div class="col-xs-4">
433                     <label for="loaded" class="control-label">Loaded</label>
434                     <input type="number" class="form-control buffer-5" id="loaded" name="loaded" value="" placeholder="00000"></input>
435                     <label id="loaded-error" class="error" for="loaded"></label>
436                   </div>
437
438                   <div class="col-xs-4">
439                     <label for="rejected" class="control-label">Rejected</label>
440                     <input type="number" class="form-control buffer-5" id="rejected" name="rejected" value="" placeholder="00000"></input>
441                     <label id="rejected-error" class="error" for="rejected"></label>
442                   </div>
443
444                   <div class="col-xs-4">
445                     <label for="dispensed" class="control-label">Dispensed</label>
446                     <input type="number" class="form-control buffer-5" id="dispensed" name="dispensed" value="" placeholder="00000"></input
447                     <label id="dispensed-error" class="error" for="dispensed"></label>
448                   </div>
449                 </div>
450   <!--
```

Figura 4 – Pantalla en formato Output del cajero automático donde indica al técnico que esta en modo de operación e indica la cantidad que hay en cada "cassette" para dispensar durante cada transacción.

Figura 5 – Pantalla en formato de operación donde indica la cantidad que haya en cada compartimiento. Los cassette verde son los compartimientos que tienen dinero y los cassette en rojo son los compartimientos que fueron vaciados.

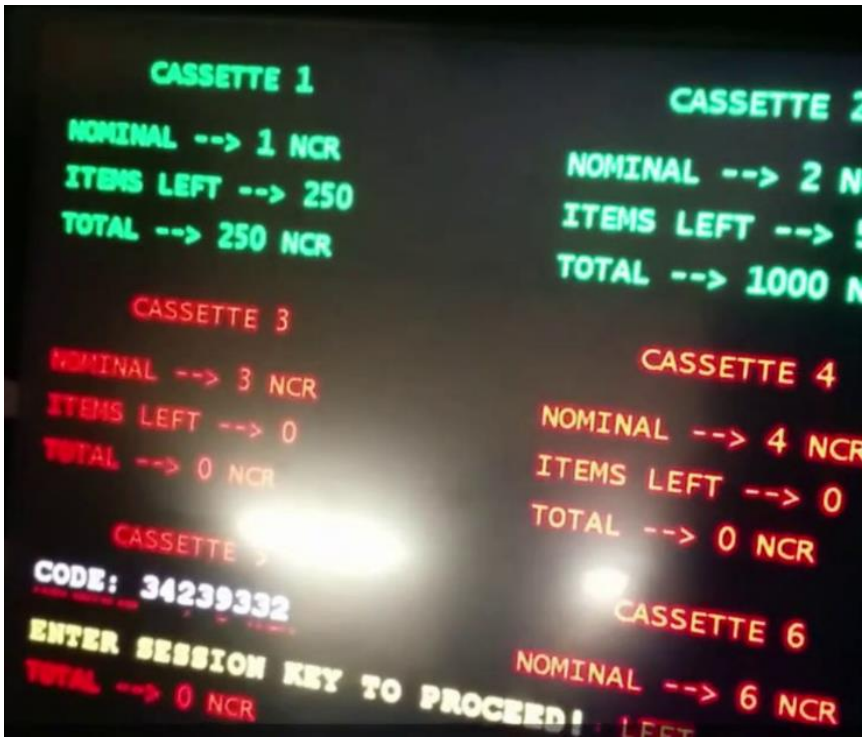


Figura 6 – Actividades encontradas en la ATM, transacciones, depósitos de los técnicos y retiros por los acusados

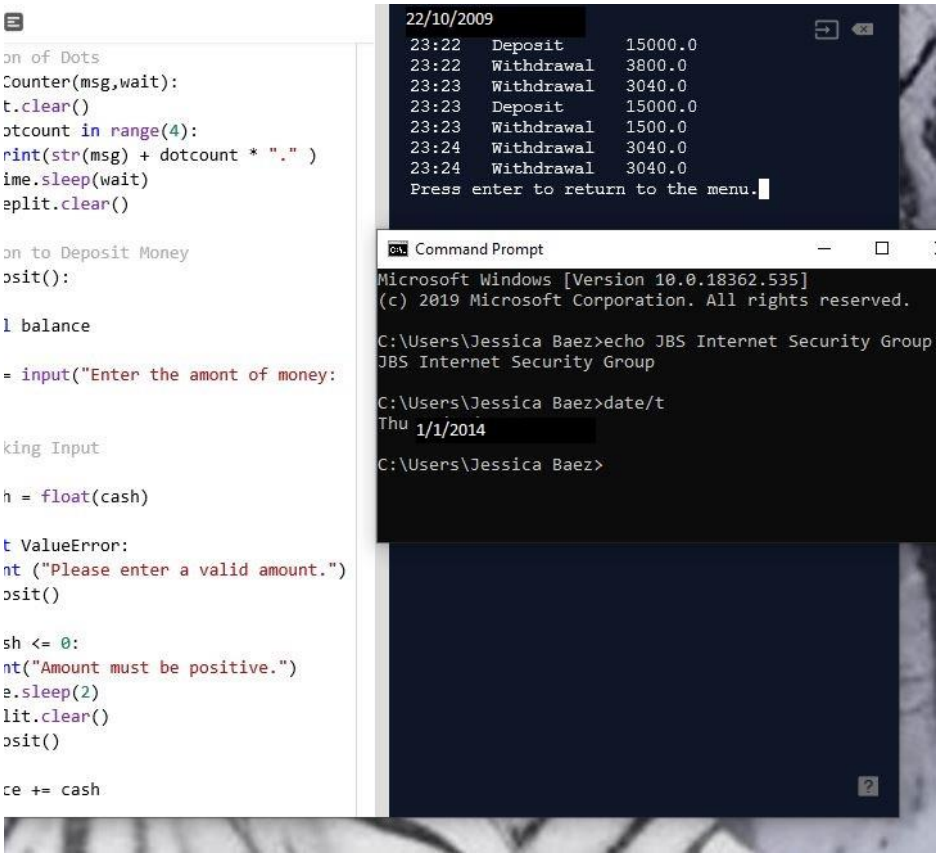


Figura 7 – Logs files encontrados de entrada y salida de los usuarios en este caso de los codigos que identifican como tecnicos.

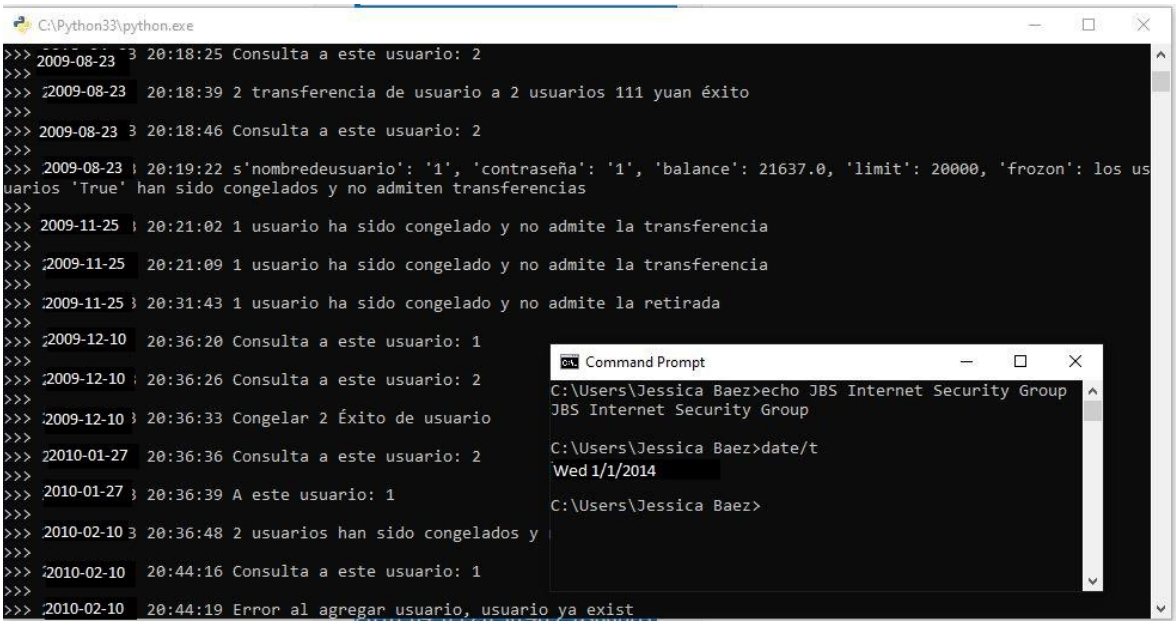
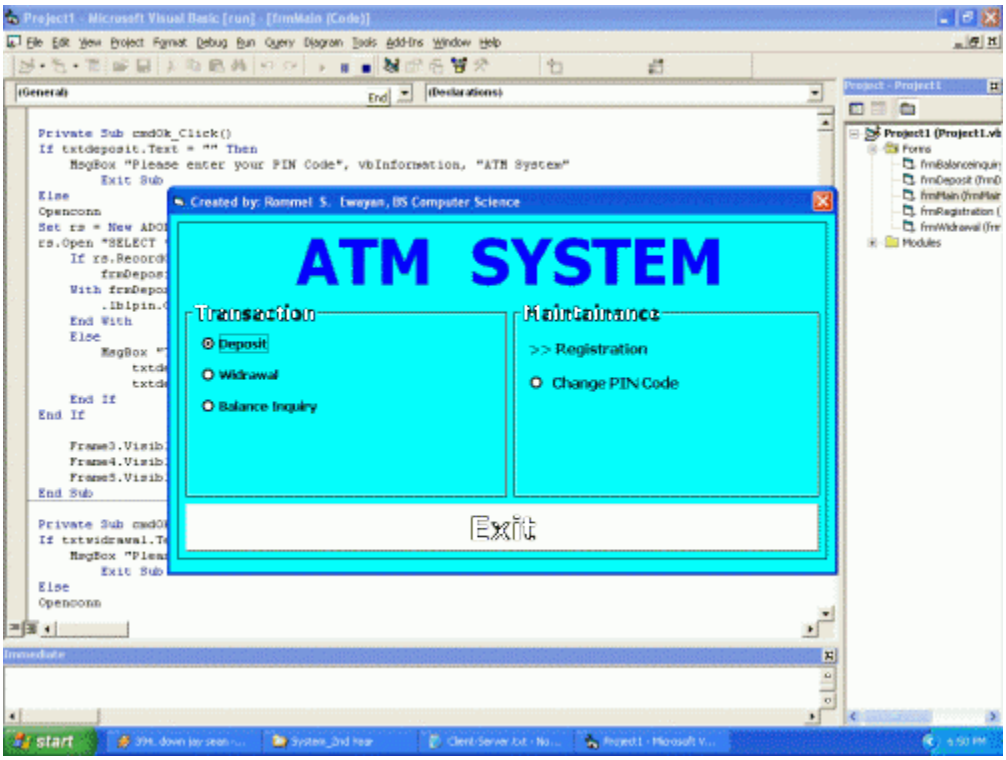


Figura 8 – Pantalla de la programación de la ATM en el formato de técnico, una vez se haya realizado la programación en formato C+, se corre el sistema para que aparezca en formato visual del cliente.



Cadena de custodia

Al comenzar nuestro proceso debemos asegurarnos de establecer una cadena de custodia de evidencia integra. La cadena de custodia se ocupa de establecer el proceso de adquisición, análisis y control de toda evidencia. En el siguiente documento se detalla la cadena de custodia seguida por JBS Internet Security Group:

Primer Evento:

- **Evidencia recogida:** Obtuvimos la primera evidencia en el cuarto de evidencias del Servicio Secreto de los Estados Unidos. La evidencia entregada fue por el fiscal Eric Rivera y recogida por Jessica Báez Sánchez, investigadora de JBS Internet Security Group. La evidencia consiste en: disco duro interno de maquina ATM modelo C4000

- **Evento verificado por:** Jessica Báez Sánchez y Eric Rivera
- **Fecha de comienzo:** 1 de enero de 2014 - 9:00 am
- **Fecha de terminación:** 1 de enero de 2014 – 10:00 am
- **Lugar de origen:** Cuarto de Evidencia Oficina Servicio Secreto de los Estados Unidos
- **Destino:** Laboratorio Forense – JBS Internet Security Group

Segundo evento:

- **Descripción del evento:** Se creó el número de caso y se le asignó el número de evidencia en nuestro sistema de investigación.
- **Evento verificado por:** Jessica Báez Sánchez
- **# de evidencia:** E-SC-2014-1-1 (E=Evidencia, SC=iniciales de la empresa 2014= año, 1-1= mes, y día de la entrega de "pruebas" por parte del cliente)
- **# del Caso** SC-2014-1-1
- **Fecha de comienzo:** 2 de enero de 2014 - 12:07 pm
- **Fecha de terminación:** 2 de enero de 2014 – 12:08 pm
- **Lugar de origen:** Laboratorio Forense – JBS Internet Security Group
- **Destino:** Laboratorio Forense – JBS Internet Security Group

Tercer evento:

- **Descripción del evento:** Se comenzó con la investigación y análisis de evidencia.
- **Evento verificado por:** Jessica Báez Sánchez
- **# de evidencia:** E-SC-2014-1-1
- **# del Caso** SC-2014-1-1
- **Fecha de comienzo:** 4 de enero de 2014 - 12:08 pm

- **Fecha de terminación:** 4 de enero de 2014 – 12:56 pm
- **Lugar de origen:** Laboratorio Forense – JBS Internet Security Group
- **Destino:** Laboratorio Forense – JBS Internet Security Group

Cuarto evento:

- **Descripción del evento:** Se analizó el dispositivo electrónico encontrando alguna evidencia en la cual necesitamos más información de parte de la compañía para poder comparar la información recopilada.
- **Evento verificado por:** Jessica Báez Sánchez
- **# de evidencia:** E-SC-2014-1-1
- **# del Caso** SC-2014-1-1
- **Fecha de comienzo:** 5 de enero de 2014 - 9:00 am
- **Fecha de terminación:** 5 de enero de 2014 – 12:30 pm
- **Lugar de origen:** Laboratorio Forense – JBS Internet Security Group
- **Destino:** Laboratorio Forense – JBS Internet Security Group

Quinto evento:

- **Descripción del evento:** Entrega de informe de análisis forense al Sr. Eric Rivera para su evaluación. El informe fue entregado directamente al fiscal Rivera por el investigador a cargo de la evidencia, Jessica Báez Sánchez
- **Evento verificado por:** Jessica Báez Sánchez y Eric Rivera
- **# de evidencia:** Reporte referente a la evidencia # E-SC-2014-1-1– Asignada al caso # SC-2014-1-1
- **Fecha de comienzo:** 7 de enero de 2014 – 9:00 am
- **Fecha de terminación:** 7 de enero de 2014 – 10:00 am

- **Lugar de origen:** Laboratorio forense – JBS Internet Security Group
- **Destino:** Oficina del fiscal federal Eric Rivera

Sexto evento:

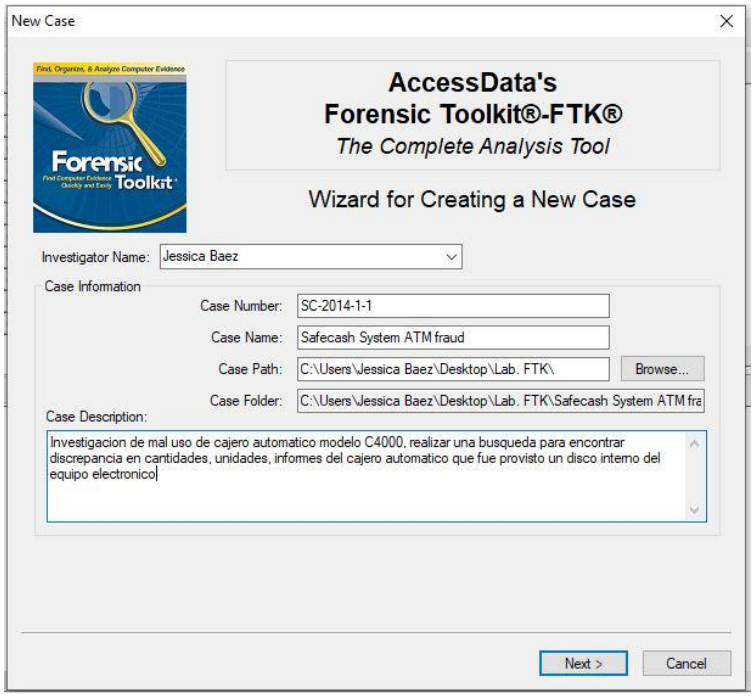
- **Descripción del evento:** Devolución de la evidencia original entregada directamente al fiscal Rivera por la investigadora a cargo Jessica Báez Sánchez.
- **Evento verificado por:** Jessica Báez Sánchez y Eric Rivera
- **# de evidencia:** E-SC-2014-1-1– Asignada al caso #SC-2014-1-1
- **Fecha de comienzo:** 8 de enero de 2014, – 9:00 am
- **Fecha de terminación:** 8 de enero de 2014 – 10:00 am
- **Lugar de origen:** Laboratorio forense – JBS Internet Security Group
- **Destino:** Cuarto de evidencias oficina Servicio Secreto de los Estados Unidos

Procedimientos

A continuación, se describen los procedimientos empleados durante el proceso de descubrimiento, adquisición, recuperación y preservación de la evidencia.

1. **Procedimiento: creación del caso**
    a. Herramienta: FTK Forensic Toolkit
    b. Fecha: 2 de enero de 2014
    c. Fecha de comienzo**:** 2 de enero de 2014– 12:07 pm
    d. Fecha de terminación**:** 2 de enero de 2014 – 12:25 am
    e. Se asigna número de caso SC-2014-1-1
    f. Descripción: **(Imagen Figura 5)**

Figura 9 - Se preparó el caso con Forensic Toolkit con toda la información para identificar el caso



2. Procedimiento: preparación de imagen

a. Captura de la imagen a ser utilizada

b. Herramienta: FTK Forensic Toolkit

c. Fecha de comienzo: 2 de enero de 2014 – 12:07 pm

d. Fecha de terminación: 2 de enero de 2014 – 12:25 pm

e. Se asigna número de evidencia E-SC-2014-1-1

f. Descripción: **(Imagen Figura 6)**

Figura 10 - Se crea la información de evidencia, se le asigna un número de evidencia sobre el caso en cuestión

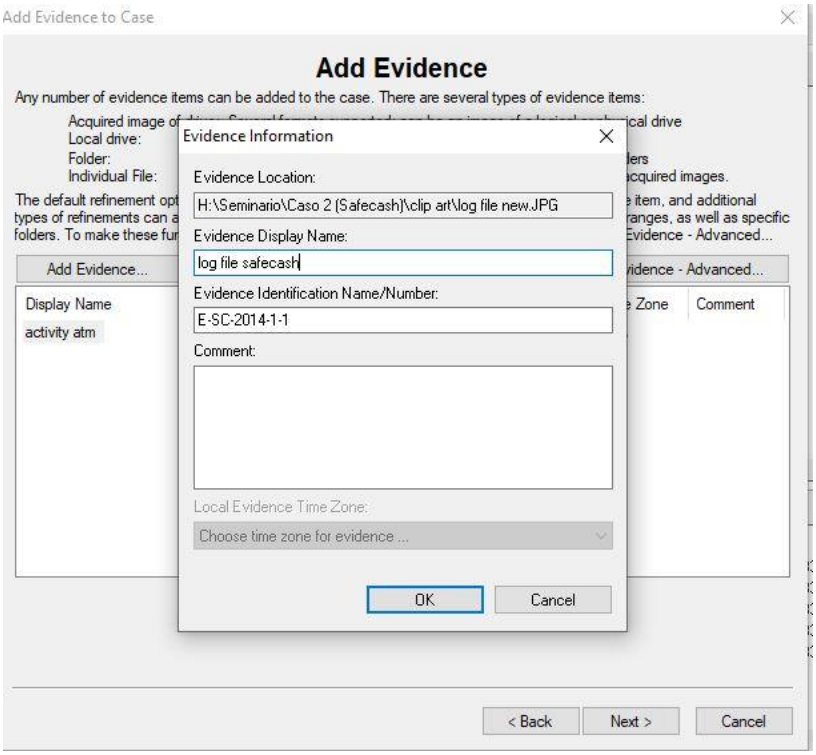
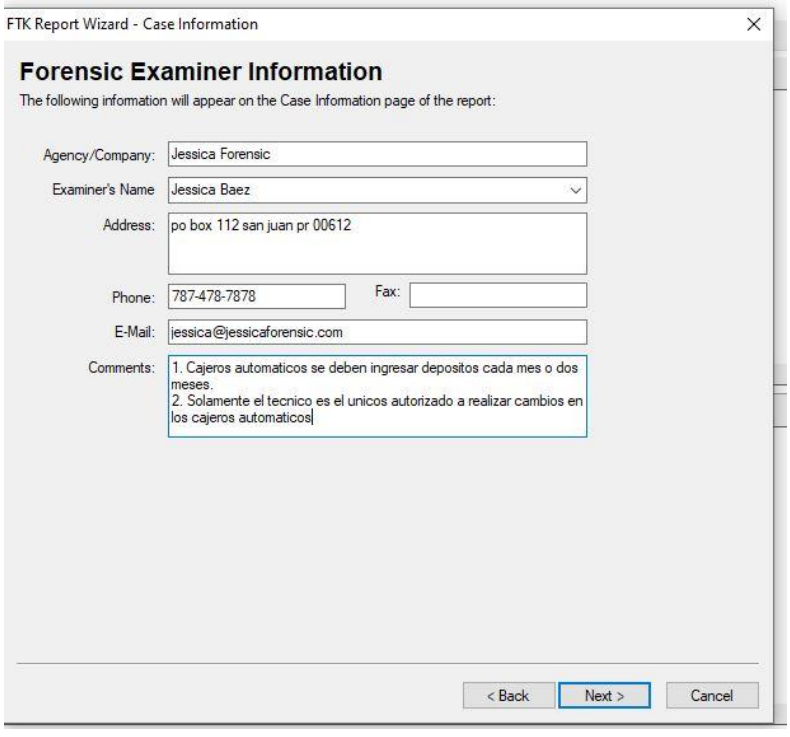


Figura 11 – Se describe la información que se esta buscando en los files que se están investigando



3. **Procedimiento: análisis de imágenes**

   a. En este punto se procesará la imagen para obtener posible evidencia inculpatoria y probar la hipótesis de fiscalía federal. Se buscarán documentos existentes y borrados (recuperación de estos).

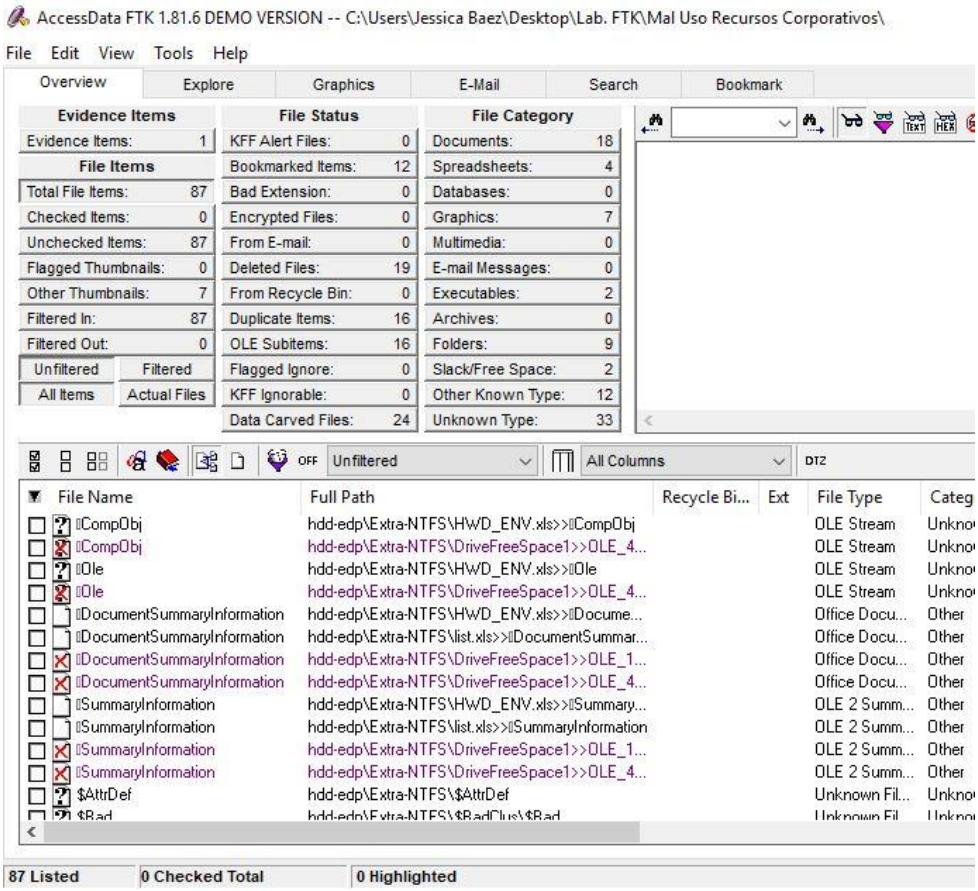
   b. Herramienta: FTK Forensic Toolkit

   c. Fecha de comienzo: 4 de enero de 2014 – 9:00 am

   d. Fecha de terminación: 4 de enero de 2014 – 12:30 pm

   e. Descripción: **(Imagen Figura 8)**

Figura 12 - Muestra total de archivos encontrados entre ellos archivos existentes y archivos borrados del dispositivo.



4. **Procedimiento: realización y determinación de bookmark**

   a. En esta parte del procedimiento, se crean bookmark (imágenes o datos importantes que se estarán evaluando a más detalle para verificar y comparar con otros programas de encontrar la misma información.

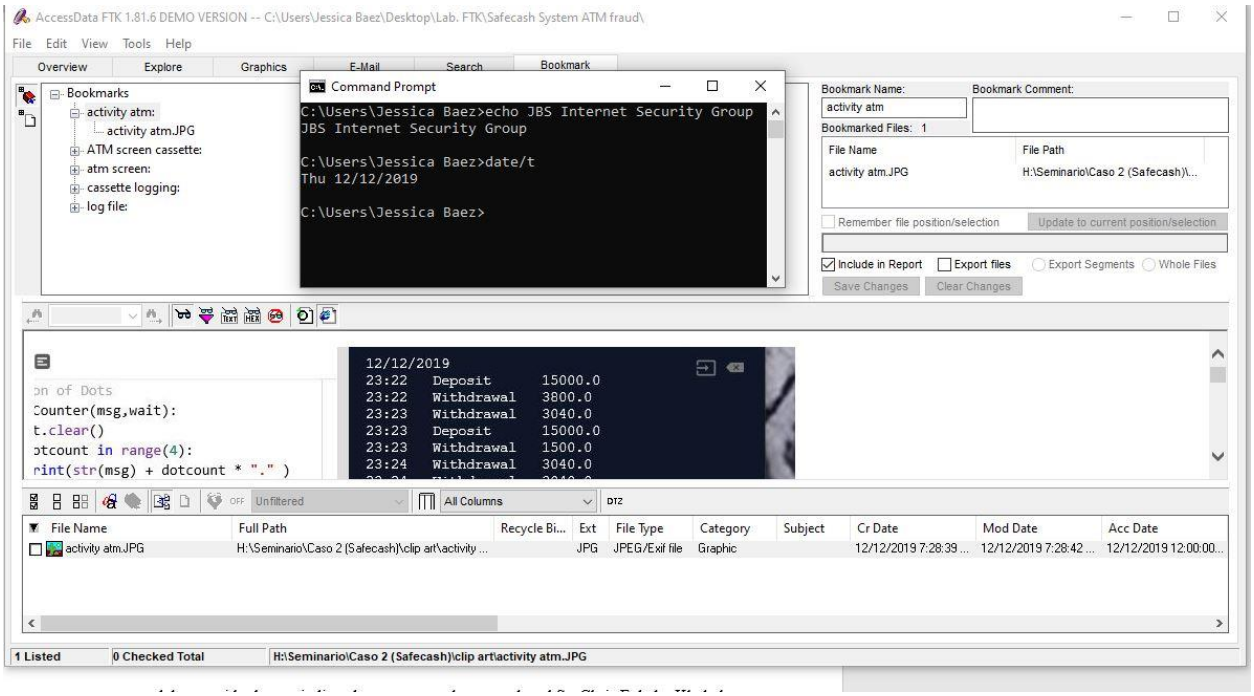
   b. Herramienta: FTK Forensic Toolkit

   c. Fecha de comienzo: 4 de enero de 2014 – 2:00 pm

   d. Fecha de terminación: 4 de enero de 2014 – 7:00 pm

   e. Descripción: **(Imagen Figura 9)**

Figura 13 - Muestra los bookmark (imágenes o datos importantes para evaluarse) donde establecemos que hemos encontrado alguna información importante para llevar el caso.



Conclusión

Luego de evaluar la evidencia encontrada en el dispositivo electrónico podemos concluir que parte del contenido de este indica claramente que los acusados el Sr. Chris Folad y Khaled Fattah están vinculados al fraude electrónico retirando dinero de los cajeros automáticos

cambiando el master key, el cual este es utilizado únicamente por el técnico que este registrado para el depósito y arreglo de los cajeros automáticos.

Está establecido que el disco duro interno no fue alterado por nadie al momento de la entrega. La cadena de custodia claramente establece que JBS Internet Security Group recogió el dispositivo del cuarto de evidencia del Servicio Secreto de los Estados Unidos bajo la supervisión del fiscal Eric Rivera y que esta evidencia fue colocada allí por los agentes que la incautaron. Existe copia de la cadena de custodia en la cual muestra con todos los detalles los procesos llevados a cabo durante toda la investigación. Se creó copia de los archivos dentro del dispositivo para mantener el dispositivo original en óptimas condiciones sin alteración.

Es por eso por lo que concluimos que toda la evidencia aquí expuesta cumple con todos los estándares de integridad y confiabilidad para ser utilizada en cualquier proceso legal. Además, certificamos que todos los procesos utilizados para la obtención de dicha evidencia cumplen o exceden los parámetros establecidos por el gobierno federal y las prácticas estándares de la industria forense digital.

Discusión del Caso

La empresa en cuestión SafeCash System perdió grandes sumas ascendientes a $600,000 por medio del fraude electrónico el cual fue realizado por los acusados antes mencionados, utilizando varias técnicas de robo, cambiando contraseñas, cambiado denominaciones de las cantidades en dólares. Existen varios tipos de fraude que son relacionados al fraude bancario utilizando cajeros automáticos ATM, algunos de estos podemos mencionar Skimming, ATM Jackpotting, Tyupkin, entre otros. Basado en nuestra investigación podemos definir que el método utilizado fue el fraude Tyupkin. Este nuevo programa, que Kaspersky Lab detecta como

Backdoor.MSIL Tyupkin, afecta a los cajeros automáticos de uno de los principales fabricantes que ejecutan Microsoft Windows 32-bit.

Tyupkin utiliza varias tácticas para mantenerse escurridizo y evitar que lo detecten. En primer lugar, sólo se activa en un momento específico de la noche. También utiliza una llave diferente que le entrega una fuente al azar en cada sesión. Sin ella, nadie puede interactuar con el cajero infectado.

Si la llave es la correcta, el programa muestra información sobre la cantidad de dinero guardada en cada cartucho y permite que un atacante con acceso físico al cajero retire 40 billetes del cartucho seleccionado.

La mayoría de las muestras que se analizaron se compilaron en marzo de 2014, mismo tiempo que los acusados utilizaron este método para el robo de dinero. Este programa ha ido evolucionando con el tiempo. En su última variante (versión. d), implementa técnicas para evitar la depuración y la emulación y desactiva McAfee Solidcore del sistema infectado.

Como funciona este malware:

> Después de cada instrucción, el operador debe presionar "Aceptar" en el teclado del cajero.
>
> Tyupkin también usa llaves de sesión para prevenir la interacción con usuarios elegidos al azar. šDespués de que se ingresa el comando para mostrar la ventana principal, el programa muestra un mensaje en inglés que dice "¡INGRESE LA LLAVE DE SESIÓN PARA PROCEDER!", con una fuente aleatoria en cada sesión.
>
> El operador malicioso debe conocer el algoritmo para generar una llave de sesión basada en la fuente que se muestra. šEl criminal debe ingresar la llave correcta para interactuar con el cajero infectado.

Al hacerlo, el programa muestra el siguiente mensaje:

OPERACIÓN DE EFECTIVO PERMITIDA.
PARA INICIAR LA OPERACIÓN DE EXPEDICIÓN –
INGRESE EL NÚMERO DE CARTUCHO Y PRESIONE ACEPTAR.

Cuando el operador selecciona el número de cartucho, el cajero expende 40 billetes de ese cartucho.

Si la llave de sesión que se ingresó es incorrecta, el programa desactiva la red local y muestra el mensaje:

DESACTIVANDO RED DE AREA LOCAL….
POR FAVOR ESPERE…..

AUDITORÍA Y PREVENCIÓN

Basado en la investigación de este tipo de fraude en la que está envuelto un cajero automático de una compañía privada y uno de sus antiguos empleados, no podemos definir en si toda su operación a través de los controles de seguridad, pero si podemos analizar su vulnerabilidad ante la entrada de seguridad de sus equipos electrónicos los cajeros automáticos que están distribuidos en diferentes ciudades y diferentes edificios para el disfrute y accesibilidad de las personas. Una incorrecta configuración del sistema operativo puede, en ocasiones generar la aparición de problemas de seguridad en el propio sistema operativo o en alguna de las aplicaciones en ejecución.

En esta investigación podemos deducir:

- Qué no tuvieron un límite en el control de transacciones dummies.
- El fraude fue continuo y además utilizaron sus propias tarjetas y cuentas para realizar el fraude. (algo que conduce a la facilidad de encontrar errores)
- El password debe ser cambiado tan pronto encontraran transacciones continuas.
- Debió presentar una alerta cada equipo cuando se realicen más transacciones del límite por equipo y presentar un informe detallado instantáneamente a su supervisor o gerente de la compañía.

Soluciones propuestas a las fallas encontradas

- Este esquema de fraude, aunque fue realizado por un aun empleado. Este debía tener un control de registro de los equipos, los cuales al final del día pudieran ser firmados y corroborados según sus sistemas, para que dieran la misma información, y desde ahí poder controlar este esquema

- Se pudo tener doble autorización para realizar cualquier movimiento en los sistemas de las ATH, una del técnico y una de su supervisor.

Trasfondo, alcance y objetivo

En este caso, su problema primordial fue tener equipos electrónicos entiéndase cajeros automáticos (ATM) obsoletos, en los cuales no cumplían con las leyes federales según se nos informó a través de los informes escritos del tribunal. Estos equipos estaban obsoletos a nivel de leyes federales los cuales no cumplen con las leyes de personas con impedimentos. Pero esto fue observado luego de que se encontró el fraude electrónico, ya que cuando los del Servicio Secreto realizaron investigaciones encontraron que la compañía SafeCash no cumplía con dichas leyes y por tanto debían proceder con el cambio de equipo y comprar o adquirir equipos nuevos que cumplieran con todas las leyes federales y además cumplan con los protocolos de seguridad para brindar acceso protegido y este no fuera objeto de otro tipo de fraude.

Además, parte de los controles de seguridad está el PCI DSS que es basado en la seguridad de las tarjetas de pago y que deben estar aprobados en los cajeros automáticos, para proteger la entidad, identidad y seguridad de los individuos. Esto se llama el estándar de seguridad de datos de la industria de tarjetas de pago (*Payment Card Industry Data Security Standard* – PCI DSS) este es un estándar de seguridad publicado por el PCI SSC y orientado a la definición de controles para la protección de los datos del titular de la tarjeta y/o datos confidenciales de autenticación durante su procesamiento, almacenamiento y/o transmisión.

La función de los cajeros automáticos debe seguir un protocolo de seguridad estos deben estar programados para conectarse con el network o con la base de información que conecta al banco para verificar transaccione, aprobar, denegar, emitir errores o enviar mensajes específicos.

Algunos de los protocolos de comunicación con el banco es la norma ISO 8583 Financial transaction card originated messages.

Algunos de estos cajeros automáticos están programados para procesar transacciones utilizando sistema operativo Windows y otros están programados con sistemas operativos en otros tipos de lenguajes que su información está cifrada y procesa las transacciones de modo cifrado. Su control de seguridad está basado en:

- Cifrado de comunicaciones (se suele usar VPN por que la comunicación del propio software no se permite cifrado por iniciativa de interoperabilidad)
- Cifrado de disco
- Protección de BIOS (es la abreviatura de Binary Input Output System, y es un software que reside en un chip instalado en la motherboard de la PC, y que realiza su tarea apenas presionamos el botón de encendido del equipo).
- Configuración de nuevos componentes (verificar que se puedan poner en producción y emitan errores si es necesario en el Journal Virtual)
- Pasar los estándares Payment Card Industry
- Compra de soluciones Antivirus.
- Gestión de parches (depende del contrato con el fabricante generalmente suelen ser a cada 3 meses los más precavidos ya que algunos fabricantes no actualizan parches cruciales.
- Correlación de eventos (básicamente esto se entiende como extraer un archivo que se llama Journal donde están los registros de todo lo que ocurre a nivel de XFS en el ATM), pero también se implementa en algunos casos a nivel de Windows.
- Gestión de contraseñas (lo administra el dueño del ATM)

- Restricción de accesos (lo administra el dueño del ATM)
- Protección de llaves acceso al software (lo administra el fabricante es su puerta de acceso)
- Actualizaciones del sistema operativo de Windows (lo administra en algunos casos el fabricante.
- Dispositivos anti skimming
- Políticas de respuesta a incidentes, políticas de detección, remediación, recuperación.
- Identificación del personal que tiene acceso (trasportadoras de valores, personal técnico interno, proveedor etc.)

Hallazgos detallados y recomendaciones

Se presentarán los hallazgos encontrados en las deficiencias que incurrió esta empresa en este caso SafeCash durante los protocolos y/o controles de seguridad que no se siguió y este permitió ocurriera el fraude.

Hallazgos	Condición	Recomendación
Transacciones dummies o transacciones realizadas por un técnico	Critica	Se debió regular las transacciones realizadas por los técnicos, estas transacciones dummies que son para verificar los equipos dispensen el dinero de forma adecuada sin errores y procesen las tarjetas que le sean introducidas.
Parches de seguridad y/o parches de sistema operativo	Critica	Estos parches ayudan a reparar los “bugs” que contengan algún tipo de error que pueda mantener vulnerable el equipo, los hackers aprovechan estas ventanas de errores para adentrarse a los equipos que más les atraiga a efectos económicos.

Contraseñas	Crítica	Estas contraseñas deben ser cambiadas cada cierto tiempo, además estas deben ser cambiadas o bloqueadas una vez un técnico de cajeros automáticos, renuncie o sea desligado de sus funciones en la empresa.
Accesos	Critica	Debe de tener restricción de accesos. Estos accesos al igual que las contraseñas deben ser cambiadas cada cierto tiempo tal vez cada 6 meses o cada vez que un técnico renuncie o se desligue de sus funciones, estos accesos también no deben ser iguales deben ser cambiantes y estos deben llevar un registro de acceso por gerenciales.
Conexión con centrales del banco	Critica	De la misma forma que los cajeros automáticos se conectan con los bancos para evaluar, aceptar las transacciones estas conexiones deben ser transmitidas automáticamente con los gerenciales de la empresa para auditorias, y no solamente se mantengan en un journal dentro del equipo.
Programas de reconocimiento de vulnerabilidad del sistema	Critica	Se debe tener un programa que proteja los sistemas contra malware y este actualice los programas o antivirus Y además deberá mantener programas que identifiquen vulnerabilidades, ventanas activas. Probar los estándares de seguridad
Supervisión de sistemas, equipos, empleados	Critica	Debe contar con supervisión constante de los equipos, empleados, transacciones que se procesen en los cajeros automáticos. Deberá rastrear y supervisar los accesos y recursos de la red y a los datos de los titulares de las cuentas y/o tarjetas.

Cumplir con las regulaciones de seguridad PCI DSS y leyes federales	Critica	En este protocolo el cajero automático debe cumplir con los requisitos de seguridad como remover los datos de autenticación de los individuos, controlar el acceso a los sistemas (controlar la introducción de la tarjeta al equipo) esto para proteger que un individuo no autorizados este usando la tarjeta.
Reportes de uso	Critica	Estos reportes deben ser diarios, estos deben ser enviados a la empresa que contenga la autorización de uso del cajero automático para tener una auditoria más completa, detallada y actualizada del uso de estos. Así podrán obtener información sobre su mal uso o el uso adecuado de los cajeros automáticos.

CONCLUSION

Luego de evaluar la evidencia encontrada, además de hacer referencia al informe de auditoría de la empresa Worldpay y además de la auditoria del Servicio Secreto de los Estados Unidos concluimos que en efecto ocurrió el fraude financiero hacia la compañía Safe Cash y uno de sus cajeros automáticos. En fin, podemos definir que esta fue la forma más fácil y rápida para ellos estafar a la empresa. Este formato clave de acceso genérico para los técnicos debe estar además regulada por los supervisores o gerente. El control Accounting es uno de los controles de seguridad que se pudiera usar para detectar algún tipo de descuadre monetario, descuadre de razones por las cuales el técnico uso la clave de acceso.

Está establecido que el disco duro utilizado en nuestras oficinas no fue alterado por nadie al momento de la entrega. La cadena de custodia claramente establece que JBS Internet Security Group recogió el dispositivo del cuarto de evidencia del Servicio Secreto de los Estados Unidos bajo la supervisión del fiscal Eric Rivera y que esta evidencia fue colocada allí por los agentes que la incautaron. Existe copia de la cadena de custodia en la cual muestra con todos los detalles los procesos llevados a cabo durante toda la investigación. Se creó copia de los archivos dentro del dispositivo para mantener el dispositivo original en óptimas condiciones sin alteración.

Es por eso por lo que concluimos que toda la evidencia aquí expuesta cumple con todos los estándares de integridad y confiabilidad para ser utilizada en cualquier proceso legal. Además, certificamos que todos los procesos utilizados para la obtención de dicha evidencia cumplen o exceden los parámetros establecidos por el gobierno federal y las prácticas estándares de la industria forense digital.

El proceso de análisis forense digital envuelve la adquisición, preservación, análisis, y presentación de evidencia digital. Este tipo de evidencia es frágil y el investigador podría, sin darse cuenta alterar, o destruir la información contenida en algún dispositivo que está siendo objeto de análisis. Esto trae como consecuencia que esta evidencia sea declarada inadmisible ante un tribunal.

Para la fecha que se produjo este fraude electrónico, estaba en auge los robos a cajeros automáticos, pero utilizando un dispositivo que leía las tarjetas o las numeraciones que se registraban, y este virus/malware llamado Tyupkin fue detectado por la empresa de seguridad que contiene un antivirus Kapersky Lab este logro obtener información de este virus/malware y este permite a los cibercriminales vaciar el dinero de cajeros automáticos mediante manipulación directa.

Este malware, detectado por Kaspersky Lab como Backdoor.MSIL.Tyupkin, afecta a cajeros automáticos de los principales fabricantes de cajeros automáticos que ejecutan Microsoft Windows de 32 bits. Actualmente los fraudes electrónicos a través de cajeros automáticos, dispositivos POS, todo equipo electrónico en el cual se use una tarjeta de banco para realizar un pago, retirar dinero y ahora depositar dinero, está siendo altamente atacado por los delincuentes ya que la venta de estas tarjetas en el darkweb está siendo mejor pagada y aun la interpol y otras agencias federales investigan sobre los usuarios que comprar y venden esta información al darkweb.

El fraude electrónico cambia todo el tiempo debido a los intrusos que buscan todo tipo de vulnerabilidades existentes para cometer un fraude. Actualmente podemos ver que los fraudes a cajeros automáticos son mediante dispositivos que se les añaden a los cajeros automáticos para clonar las tarjetas.

En conclusión, para mí como para otros usuarios de estos cajeros automáticos ha levantado bandera para estar más atentos al momento de hacer uso. Como método de seguridad, aunque no estoy exenta es no usar los cajeros automáticos privados que se encuentran en puestos de gasolina, siempre trato de usar los que son de bancos. Además, siempre trato de revisar los dispositivos que se encuentran en el cajero, siempre que tengo tiempo, me encuentro segura en el lugar porque tal vez no tenga un dispositivo en el cajero, pero si tenga un delincuente velando el lugar para un asalto.

REFERENCIAS

- ATM 'Jackpotting' Attacks Reveal Deeper Problems (febrero 12, 2018) Recuperado de https://www.forbes.com/sites/jasonbloomberg/2018/02/12/atm-jackpotting-attacks-reveal-deeper-problems/#4a436f8b6fc3
- FTK Forensic Toolkit. (n.d.).
- Los fraudes más comunes en los cajeros automáticos y como evitarlos (octubre 3, 2018 Recuperado de https://cronicaglobal.elespanol.com/business/fraudes-cajeros-automaticos_126518_102.html
- Tyupkin: Un programa malicioso que manipula cajeros automáticos (octubre 7, 2014) Recuperado de https://securelist.lat/tyupkin-un-programa-malicioso-que-manipula-cajeros-automticos/66352/
- United States v. Chris Sohail Folad and Khaled Nabil Abdel Fattah Indictment. (22 de octubre de 2014) Recuperado de https://archive.org/details/pdfy-IGw8eZW7NkO0vmhI

- United States v. Chris Suhail Folad and Khaled Nabil Abdel Fattah Order 17 5538 17 5544. (s.f.). Recuperado de https://law.justia.com/cases/federal/appellate-courts/ca6/17-5544/17-5544-2017-12-11.html
- United States v. Chris Suhail Folad and Khaled Nabil Abdel Fattah. Transcript of proceedings, mayo, 16, 2016). Recuperado de www.pacer.com
- United States v. Chris Suhail Folad and Khaled Nabil Abdel Fattah. (s.f.). (18 de diciembre de 2018, Recuperado de https://www.morelaw.com/verdicts/case.asp?s=TN&d=98256
- United Statesv Ercan Findikoglu Indictment (25 de julio de 2013) Recuperado de https://www.justice.gov/opa/file/482256/download
- USA v Zhang Qiaocheng and Zhang Xioalang Criminal Complaint (9 de julio de 2018) Recuperado de https://www.courtlistener.com/recap/gov.uscourts.cand.329276/gov.uscourts.cand.329276.1.0.pdf