EDP UNIVERSITY OF PUERTO RICO, INC.
RECINTO DE HATO REY

PROGRAMA DE MAESTRÍA EN SISTEMA DE INFORMACIÓN CON ESPECIALIDAD
EN SEGURIDAD E INFORMACIÓN DE FRAUDE

FROM PHISHING TO CARDING
UN CIBERATAQUE BASADO EN LA INGENIERIA SOCIAL

REQUISITO PARA LA MAESTRÍA EN SISTEMA DE INFORMACIÓN CON
ESPECIALIDAD EN SEGURIDAD E INFORMACIÓN DE FRAUDE

Diciembre, 2021

PREPARADO POR
CORAL N. BAUTISTA LIZ

Sirva la presente para certificar que el proyecto de investigación titulado:

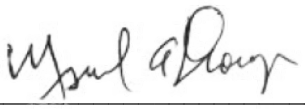
FROM PHISHING TO CARDING
UN CIBERATAQUE BASADO EN LA INGENIERIA SOCIAL

PREPARADO POR
CORAL N. BAUTISTA LIZ

Ha sido aceptado como requisito principal para el grado de maestría en sistema de información con especialidad de información e investigación de fraude.

Diciembre, 2021

Aprobado por:



Dr. Miguel A. Drouyn Marrero, Profesor

Tabla de Contenido

Tabla de Figuras

INTRODUCCIÓN Y TRASFONDO

Introducción

Para el estudio del caso en cuestión, se hace un acercamiento de delitos informáticos, en donde se involucra al hacker ruso Aleksey Burkov quien fue arrestado en el año 2015 en el aeropuerto Ben Gurion después de haber sido acusado de fraude con tarjetas de crédito de los Estados Unidos. Si bien, este caso se refiere a que para los años 2009 y 2013 Burkov dirigió un sitio web clandestino que vendía datos de tarjetas de crédito, más de 150.000, las cuales pertenecían a ciudadanos estadounidenses. La relevancia de este caso y de los delitos cometidos, se basa en los daños al patrimonio causado, los cuales oscilan entre los 20 millones de dólares y por la seguridad pública.

Descripción del caso

Número del caso: 1:15-cr-00245-TSE-1

Partes en el caso:

- Acusado: Aleksei Yurievich Burkov
- Víctimas: Ciudadanos de EE. UU.
- Investigadores: Deparment of Justice of United State of America
- Abogado: Gregory E. Stambaugh | Abogado criminalista
- Fiscales: Kellen Dwyer | Fiscal federal | *U.S. District Court for the Eastern District of Virginia, Alexandria Division.*
- Juez: Thomas Selby Ellis III | *Senior United States District Judge of the United States District Court for the Eastern District of Virginia.*

Trasfondo

Alexei Burkov es un ciudadano ruso que fue extraditado a Estados Unidos desde Israel. Burvok fue acusado por fraude electrónico, fraude de dispositivos de acceso y conspiración para cometer fraude electrónico, intrusiones informáticas ilegales, fraude de dispositivos de acceso, intrusiones informáticas ilegales, lavado de dinero y robo de identidad. (Schwartz, F., & Volz, D. 2019)

Según *The Department of Justice (2020),* Burkov administraba un sitio web llamado "Cardplanet" en donde vendía números de tarjetas de pago que habían sido inicialmente robada por intrusiones informáticas. Estas tarjetas eran vendidas y pertenecía a estadounidense. Además, se habla sobre la administración de otro sitio web que hacía las veces de club en donde los ciberdelincuentes de élite entraban a anunciar bienes robados, tales como información personal y software malicioso. Dicha membresía fue creada por Burkov para garantizar que la policía no accediera a dicho foro y los miembros cumplieran con los acuerdos pactados en el negocio.

Acorde a periódico The times of Israel (2019) se recibió la denuncia en la corte superior de Jerusalén, la cual habida sido emitida en 2015 por la Interpol. Luego un tribunal del distrito israelí aprobó su extradición en 2017.

Descripción de hechos

Entre los años 2009 y 2013, el acusado Burvok, dirigió un sitio web clandestino que vendía datos de unas 150.000 tarjetas de créditos que eran pertenecientes en su mayoría a ciudadanos estadounidense. Según las víctimas, los daños patrimoniales oscilaban entre los 20 millones de dólares. (*Department of Justice, 2020)*

Desde al menos principios de 2009 hasta al menos agosto de 2013, BURKOV controló y operaba una tienda en línea de tarjetas de pagos obtenidas ilícitamente, mejor conocida como

Cardplanet LLC y Cardplanet.cc ("Cardplanet"), a través del sitio web www.Cardplanet.ee (el "Sitio web de Cardplanet"). El Cardplanet Sitio web, que contenía la interfaz de usuario para los clientes que compraron datos de tarjetas de pago robadas, estaba alojado en un servidor ubicado fuera de los Estados Unidos. Cardplanet vendió datos de tarjetas de pago por prácticamente todas las principales tarjetas de pago de EE. UU. (USA v. Alexsei Yurievich Burkov, 2015)

A. El 13 de noviembre de 2011 o alrededor de esa fecha, BURXOV realizó una publicación en un foro de tarjetas en ruso que anunciaba el sitio web de Cardplanet como proveedor de "Tarjetas CVV2 & DUMPS ". La publicación indicaba que los precios de las" Tarjetas CVV2 "estaban entre $ 2.5 y $ 10 por tarjeta, mientras que el precio de los "vertederos" oscilaba entre $ 12 y $ 35.
B. El 17 de noviembre de 2011 o alrededor de esa fecha, BURKOV hizo otra publicación en otro foro de tarjetas en ruso para promover el sitio web de Cardplanet. Esa publicación indicó que Cardplanet utilizaba facturación automatizada a través de WebMoney y Liberty Reserve, tenía una buena selección de tarjetas y vertederos, y precios basados en la demanda del mercado.
C. El 3 de febrero de 2012 o alrededor de esa fecha, un cómplice no identificado como acusado en este documento participó en una transacción financiera en un restaurante de comida rápida en Richmond, Virginia, en el Distrito Este de Virginia, utilizando una tarjeta de crédito para pequeñas empresas falsificada Company codificada con datos de tarjetas robadas vendidos en el sitio web de Cardplanet.
D. El 15 de marzo de 2013 o alrededor de esa fecha, un cómplice no identificado como acusado en este documento participó en una transacción financiera en una tienda de conveniencia en Fredericksburg, Virginia, en el Distrito Este de Virginia, utilizando

otra tarjeta de crédito Company-1 falsificada codificada con datos de tarjetas robadas vendidos en el sitio web de Cardplanet.

E. El 3 de diciembre de 2013 o alrededor de esa fecha, BURKOV vendió datos robados por seis créditos tarjetas a un agente encubierto a través del sitio web de Cardplanet.

Acusaciones, Cargos y Penalidades

A continuación en detalle los delitos que se le atribuyen al acusado(s), incluya el título y código de ley que aplica;

1. Conspiración para confirmar el acceso: Fraude de dispositivos – (18. U.S.C. § 1029 (b)(2))

   Este cargo se suscitó principalmente con la publicación y el foro que se hizo para recopilar información y datos robados.

2. Fraude de dispositivo de acceso: (18. U.S.C. § 1029 (a))

   Traficaron y utilizaron accesos no autorizados con el fin de defraudar, tales como números de cuenta, valores de verificación de tarjetas.

3. Conspiración para cometer fraude electrónico: (18. U.S.C. § 1349)

   Este cargo se imputó por confederar, conspirar y estar de acuerdo para idear un plan y un artificio para defraudar a personas conocidas y desconocidas.

4. Fraude electrónico: (18. U.S.C. § 1343 (2)(a))

   Se imputa por idear y defraudar para obtener dinero y propiedad, afectando las instituciones financieras a través de falsas promesas. A demás por ejecutar un esquema y artificio para transmitir por medio de comunicación por cable en interestatal y extranjero de comercio y vender información privada.

Definición de términos

Carding: Se refiere a diversas actividades delictivas asociadas con el robo de información financiera e información de identificación personal que pertenezca a otras personas, incluida la información asociada con tarjetas de pago (Crédito, o débito) y usar esa información para obtener dinero, bienes o servicios sin la autorización o consentimiento de las víctimas.

CVV: por sus siglas en inglés, hace referencia al termino *Card Verification Value.* Este es un código de verificación numérico de seguridad, formado por tres o cuatro dígitos, vinculado a una tarjeta de pago.

CVC: Es otro termino para definir el concepto de *Card Verification Code*, Este al igual es un código de verificación numérico, vinculado a tarjetas de pago, ubicado en el revés de la tarjeta.

Volcado: Copia no autorizada de toda la información y contenido en la banda magnética de una tarjeta de crédito activa.

REVISIÓN DE LITERATURA

Introducción

Con el desarrollo del presente trabajo se realiza una investigación cercana al caso "Aleksei Burkov vs. EE. UU." y los delitos informáticos por los cuales fue acusado. De esta manera se pretende desarrollar en un primer momento, el desglose de los fraudes involucrados con el fin de desarrollar un resumen objetivo y lógico de conocimiento sobre dichos fraudes, posteriormente, se hace una explicación de las leyes aplicables en el caso en cuestión, las cuales fueron traídas a colación con anterioridad, para posteriormente presentar de manera concreta tres casos similares al que se estudia.

Para el estudio del caso en cuestión, se hace un acercamiento de delitos informáticos, en donde se involucra al hacker ruso Aleksey Burkov quien fue arrestado en el año 2015 en el aeropuerto Ben Gurion después de haber sido acusado de fraude con tarjetas de crédito de los Estados Unidos. Si bien, este caso se refiere a que para los años 2009 y 2013 Burkov dirigió un sitio web clandestino que vendía datos de tarjetas de crédito, más de 150.000, las cuales pertenecían a ciudadanos estadounidenses. La relevancia de este caso y de los delitos cometidos, se basa en los daños al patrimonio causado, los cuales oscilan entre los 20 millones de dólares y por la seguridad pública. Alexei Burkov es un ciudadano ruso, que fue extraditado a Estados Unidos desde Israel. Burvok fue acusado por fraude electrónico, fraude de dispositivos de acceso y conspiración para cometer fraude electrónico, intrusiones informáticas ilegales, fraude de dispositivos de acceso, intrusiones informáticas ilegales, lavado de dinero y robo de identidad.

Fraudes involucrados

Fraude cibernético e informático: El Cornell Law School (s.f.), ha definido el fraude cibernético o informático como aquel fraude que se realiza por medio del uso del internet o de

una computadora. Así entonces, se hace referencia a la piratería informática o hacking como se conoce comúnmente, la cual es una forma de fraude común en la sociedad; en esta el delincuente utiliza una serie de herramientas tecnologías con el fin de poder tener acceso remoto a otra computadora con información confidencial. Así mismo, este involucra la intercepción de transmisión electrónica, permitiendo el paso al robo de contraseñas, números de cuenta de tarjetas de crédito o débito y otro tipo de información confidencial y relevante sobre la identidad de una persona.

Por su parte, la ley federal le da una definición al fraude electrónico 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. Con esto, se busca distorsionar los datos, de diversas formas tales como, alterar los datos ingresados en la red, alterar o borrar información almacenada, reescribir códigos de software y cargarlos a una computadora central de un banco para robar identidades de los usuarios.

En la siguiente tabla se hace una relación de las víctimas de fraude electrónico clasificadas por edad en el año 2020 en los Estados Unidos.

Victims		
Age Range[7]	Total Count	Total Loss
Under 20	23,186	$70,980,763
20 - 29	70,791	$197,402,240
30 - 39	88,364	$492,176,845
40 - 49	91,568	$717,161,726
50 - 59	85,967	$847,948,101
Over 60	105,301	$966,062,236

Figura 1: Victimas por edad de fraude informático en el año 2020 en EE. UU.

Nota: Federal Bureau of Investigation. (2020)

De esta manera se observa que las víctimas más frecuentadas son los mayores de 60 años, sin embargo, se presenta en todos los casos pérdidas monetarias millonarias suscitadas por este crimen.

Por su parte el FBI para el primer trimestre del año 2020 reportó más de 3.600 denuncias de fraude cibernético que se relacionaban con el COVID-19 dejando al descubierto que este delito se presenta con fines lucrativos, buscando robar la propiedad intelectual y otros aspectos relevantes en línea.

Por otro lado, dentro de las modalidades de la comisión del delito se presentan con más frecuencia el bloqueo de páginas web, en donde se adentran en las web de diferentes instituciones ya sean públicas o privadas por un tiempo determinado para producir caos, incertidumbre y confusión; la propagación de *malware*, en donde se imparte un virus, caballo de Troya, *backdoor*, programas espías entre otros para irrumpir en la información de los dispositivos; difamación e información falsa, lo cual se hace a través de sitios web en donde se daña la dignidad de las víctimas de forma considerable; robo de identidad, esto se trata de los ataques de suplantación de la identidad, las cuales se denominan como IP *Spoofing* con la cual se modifica la cabecera de los paquetes enviados a un sistema informático para simular que fueron enviados de un equipo distinto del que verdaderamente se envió; y finalmente se encuentra el espionaje informático; el cual, hace referencia a la obtención de datos almacenados en un fichero automatizado de manera no autorizada, para lo que se utilizan técnicas como *Wire Tapping* o la recogida de información residual (Fuentes. 2008).

En 2020, el IC3 recibió 2.474 quejas identificadas como *ransomware* con pérdidas ajustadas de más de $ 29,1 millones. El *ransomware* es un tipo de software malintencionado, o *malware*, que cifra los datos en una computadora haciéndolo inutilizable. Un ciberdelincuente malintencionado retiene los datos como rehenes hasta que se pague el rescate.

Si no se paga el rescate, los datos de la víctima sigue no disponible. Los ciberdelincuentes también pueden presionar a las víctimas para que paguen el rescate amenazando con destruir los datos de la víctima o con liberarlos para el público.

Por otra parte, se encuentran las campañas de phishing por correo electrónico en donde el ciberdelincuente envía un correo electrónico que contiene un archivo o enlace malicioso que despliega *malware* cuando un destinatario hace clic en él. Los ciberdelincuentes han utilizado históricamente estrategias de spam genéricas y de amplia base para implementar su *malware*, a través de las campañas de *ransomware* las cuales han sido más específicas y sofisticadas. Los criminales también pueden poner en peligro la cuenta de correo electrónico de una víctima mediante el uso de *malware* precursor, que habilita el ciber criminal para usar la cuenta de correo electrónico de la víctima para propagar aún más la infección

Fraude y dispositivos de accesos: En esta oportunidad, la ley federal constituye los delitos de actividades que usen de modo ilegítimo los dispositivos de acceso, tales como contraseñas, tarjetas, códigos, números seriales entre otros, para obtener dinero, servicios o bienes de forma fraudulenta (18 USC § 1029).

Por su parte, la USA PATRIOT expandió su aplicación fuera de la jurisdicción de los EE. UU, siempre que el delito y su comisión involucrara un dispositivo que hubiere sido cometido en su país, y que el imputado hubiere enviado, almacenado o transportado a otro país para la comisión del delito. BNC. (2019).

Intrusión Informática Ilegal: Con esta, según Móstoles, R (2019) se hace referencia al acceso ilícito a sistemas informáticos, con el cual se abre paso a la comisión de otros delitos como estafa y daños informáticos.

Una de las metodologías utilizadas en este delito es el fraude de soporte técnico el cual es un problema creciente. Este esquema involucra a un delincuente que afirma proporcionar al

cliente, seguridad o soporte o servicio técnico para defraudar a personas involuntarias. Los delincuentes pueden hacerse pasar por representantes de apoyo o servicio que se ofrecen a resolver problemas como correo electrónico o cuenta bancaria comprometida, un virus en una computadora o la renovación de una licencia de software. Las quejas recientes involucran a delincuentes que se hacen pasar por servicios de atención al cliente para instituciones financieras, empresas de servicios públicos o casas de cambio de moneda virtual. Muchas víctimas informan que se les ordenó realizar transferencias bancarias a cuentas en el extranjero o compra grandes cantidades de tarjetas de crédito.

En 2020, el IC3 recibió 15,421 quejas relacionadas con el fraude de soporte técnico de víctimas en 60 países. Las pérdidas ascendieron a más de $ 146 millones, lo que representa un aumento del 171% en pérdidas del 2019. La mayoría de las víctimas, al menos el 66 por ciento, informan tener más de 60 años y experimentar al menos 84% de las pérdidas, es decir, más de $ 116 millones en su equivalente.

Leyes aplicables

1. (18. USC § 1029 (b)(2)): Conspiración para confirmar el acceso: fraude de dispositivos. Este delito puede tener como penalidad hasta 7.5 años de prisión.

   La ley federal considera como delito actividades que utilicen de un modo ilegítimo “dispositivos de acceso” tales como tarjetas, códigos, números seriales y contraseñas, para obtener dinero, bienes, servicios u otros valores de modo fraudulento.

   Este cargo se suscitó principalmente con la publicación y el foro que se hizo para recopilar información y datos robados.

2. (18. USC § 1029 (a)(2) & 2(a)): Fraude de dispositivos de acceso

   Su penalidad comprende una multa bajo el título y prisión hasta por 10 años.

   De acuerdo con el título (18. USC § 1029) de la ley federal, este se trata de un delito con la intención de usar, producir, defraudar, producir o traficar en dispositivos de acceso

falsificados, es decir, en tarjetas códigos, placas, números de serie electrónicos, números de cuenta, números de identificación móvil, números de identificación personal u otros tipos de acceso a cuentas en las que se obtenga bienes, servicios, dinero o cosas de valor. Así mismo, en este estatuto se aplica para las tarjetas de cajero automático, tarjetas de gasolina y cualquier medio de "pago plástico".

3. (18. USC § 1349): Conspiración para cometer fraude electrónico

Este delito se imputa cuando una persona que no ha cometido en sí el acto de fraude requerido de condena por fraude electrónico, se le acusa por conspiración para cometer fraude, siempre y cuando exista evidencia acusatoria, es decir, que existió un acuerdo para cometer fraude a través de medios electrónicos o correo.

Incluso si una persona no tomó la acción abierta, puede ser acusada de conspiración. Según la ley federal, es suficiente que un acusado se una a sabiendas a una conspiración en la que el uso del correo o la comunicación electrónica podría haber promovido la conspiración y que al menos una de las partes involucradas haya tomado una acción abierta. De hecho, una vez que se haya establecido oficialmente la participación de un acusado en una conspiración, el acusado será considerado culpable de cualquier acto cometido por sus supuestos socios, incluso si el acto abierto fracasó. Tampoco es necesario que alguien supuestamente coconspirador conozca al resto de los conspiradores para ser considerado parte del grupo.

4. (18. USC §§ 1343 & 2(a)): Fraude electrónico

Impone una pena de hasta 20 años de prisión.

El fraude electrónico tiene como objetivo obtener un beneficio de forma ilegal sin beneficiar al consumidor. El fraude electrónico incluye casi cualquier delito basado en el fraude, que incluye, entre otros, fraude hipotecario, fraude de seguros, fraude fiscal, robo

de identidad, sorteos, fraude de lotería y fraude de telemercadeo. En esta oportunidad la ley federal funciona de forma conjunta con el estatuto de fraude postal.

Casos relacionados

USA vs. Meigss y Harrington (2019)

Cargos: Conspiración para cometer fraude informático y abuso y fraude electrónico (18U.S.C.§371). Fraude electrónico; Ayudar y apostar (18 U.S.C.§§ 1343 y 2). Fraude y Abuso Informático; Ayuda) y Apuestas) (18 U.S.C.§§ 1030 (a) ((2), (c) (2) (B) (ii) y 2). Robo de Identidad Agravado; Ayudar y apostar (18 U.S.C.§§ 1028A y 2). Alegación de decomiso (18 U.S.C.§§ 371, 981 (a) (l) (C)

Se acusan a dos hombres por llevar a cabo un plan para hacerse cargo de las cuentas de redes sociales de las víctimas y robar criptomonedas utilizando técnicas como “intercambio de SIM”, piratería informática y otros métodos. Fueron acusados con 11 cargos, entre los que se encuentran conspiración, fraude electrónico, fraude informático y abuso y robo de identidad agravado. Según la acusación, Meiggs y Harrington presuntamente apuntaron a ejecutivos de compañías de criptomonedas y otros que probablemente tenían cantidades significativas de criptomonedas y aquellos que tenían nombres de cuentas de redes sociales de alto valor o "OG" (jerga para "Original Gangster"). Meiggs y Harrington supuestamente conspiraron para piratear y tomar el control de las cuentas en línea de estas víctimas para que pudieran obtener cosas de valor, como criptomonedas. Utilizaron una práctica ilegal conocida como "intercambio de SIM" y otras técnicas para acceder, tomar el control y, en algunos casos, robar criptomonedas de las cuentas. Al menos a 10 víctimas identificadas en todo el país. Los miembros de la conspiración robaron, o intentaron robar, más de $ 550,000 en criptomonedas solo de estas

víctimas. Meiggs tomó el control de las cuentas “OG” de dos víctimas con compañías de redes sociales. USA vs. Erick Meiggs and Declan Harrington. (2019)

USA vs. Alla Witte (2021)

Cargo: víctimas de delitos múltiples según las disposiciones de 18 U.S.C. 3771 (d)(2).

Se trata de una mujer de 55 años quien es acusada de 19 cargos de acusación formal, y se le acusa de participar en una organización criminal conocida como *Trickbot Group* que implementa el *malware Trickbot*. “Esta acusación demuestra el amplio alcance del Grupo de Trabajo sobre *Ransomware* y Extorsión Digital del Departamento de Justicia”, dijo la Fiscal General Adjunta Lisa O. Monaco “*Trickbot* infectó millones de computadoras víctimas en todo el mundo y se utilizó para recopilar credenciales bancarias y entregar *ransomware.* El acusado está acusado de trabajar con otros miembros de la organización delictiva transnacional para desarrollar e implementar un conjunto digital de herramientas de *malware* que se utilizan para atacar a empresas e individuos de todo el mundo para el robo y el rescate.

Estos cargos sirven como una advertencia para los posibles ciberdelincuentes de que el Departamento de Justicia, a través del Grupo de Trabajo de *Ransomware* y Extorsión Digital y junto con nuestros socios, utilizará todas las herramientas a nuestra disposición para alterar el ecosistema ciberdelincuente. “Witte y sus asociados están acusados de infectar decenas de millones de computadoras en todo el mundo, en un esfuerzo por robar información financiera para, en última instancia, desviar millones de dólares a través de sistemas informáticos comprometidos", dijo el agente especial a cargo Eric B. Smith del campo de Cleveland del FBI. Oficina. "Las intrusiones cibernéticas y las infecciones de *malware* requieren mucho tiempo,

experiencia y esfuerzo de investigación, pero el FBI se asegurará de que estos piratas informáticos rindan cuentas, sin importar dónde residan o cuán anónimos crean que son".

Witte está acusada de un cargo de conspiración para cometer fraude informático y robo de identidad agravado; un cargo de conspiración para cometer fraude bancario y por cable que afecte a una institución financiera; ocho cargos de fraude bancario que afectan a una institución financiera; ocho cargos de robo de identidad agravado y un cargo de conspiración para cometer blanqueo de capitales.

La acusada fue procesada ante el juez federal William H. Baughman Jr. del Tribunal de Distrito de los Estados Unidos para el Distrito Norte de Ohio. Si es declarada culpable, enfrenta una pena máxima de cinco años de prisión por conspiración para cometer fraude informático y robo de identidad agravado; 30 años de prisión por conspiración para cometer fraude electrónico y bancario; 30 años de prisión por cada fraude bancario sustancial; una sentencia obligatoria de dos años por cada delito de robo de identidad agravado, que debe ser cumplida consecutivamente a cualquier otra sentencia; y 20 años de prisión por conspiración para cometer blanqueo de capitales. Un juez de un tribunal de distrito federal determinará cualquier sentencia después de considerar las Pautas de Sentencia de EE. UU. Y otros factores estatutarios. (USA vs. Alla Witte, aka Max. (2021)

Herramienta de investigación

Como herramienta de investigación se utilizará *FTK Imager* la cual corresponde a una herramienta que proporciona velocidad, facilidad de uso tanto para llevar a cabo investigaciones forenses como para la captura grafica de los registros para posteriormente evaluar. Es decir FTK Imager es una herramienta ampliamente utilizada en la investigación forense que como parte de la investigación se empleara para el proceso de colección de y a examinación las pruebas adquiridas.

Esta herramienta permite que se recopilen datos de cualquier sistema digital o dispositivo en el que se produzca, almacenen o transmitan datos y además realiza el análisis forense de los mismos. Su interfaz es intuitiva y su análisis de correo electrónico, las vistas de datos, la velocidad de procesamiento y la estabilidad caracterizan la eficacia de esta.

Con esta herramienta se obtiene una solución de investigación digital. Cuenta consigo una base de datos compartida en donde toda la evidencia digital queda almacenada en esta y brinda así a los equipos, gran acceso de la evidencia reciente del caso haciendo que se reduzca tiempo, costo y complejidad; Garantizando la integridad de la recopilación de evidencia.

SIMULACIÓN DEL CASO

Introducción

En el siguiente documento se estará llevando a cabo una simulación sobre las posibles técnicas utilizadas por Aleksei Burkov. El objetivo de la exposición consiste en explicar mediante un diagrama, las metodologías utilizadas para llevar a cabo el fraude. Se deduce Burkov ataco mediante técnicas conocidas como phishing logrando acceso a los servidores de bases de datos de empresas como Banknet y Visanet ubicados en las afueras de Estados Unidos, para extraer información relacionadas a números de cuentas de pago (débito y, o crédito) valores de códigos de verificación de tarjetas (CVV o CVC), número de cuenta, fecha de vencimiento y nombre del titular; además de vender la data sustraída de las bases de datos las cuales accedió ilegalmente mediante técnicas de restauración o *Backup*.

Para llevar a cabo su plan, Burkov creo el escenario perfecto con técnicas como ingeniería social y OSINT para identificar el objetivo. Herramientas como *Maltego*, facilitarían el proceso para la búsqueda del objetivo, con fines de investigar la estructura de la organización y poder ejecutar exitosamente el fraude. Se presume que una vez este estructuro la logística del esquema procedió a ejecutar el plan de *Spear Phishing* para inducir a la víctima a instalar una actualización de los drivers para correcciones en la aplicación de manejo de base de datos. Posteriormente, se identifica la posibilidad del uso de *Metasploit* para ejecutar los códigos maliciosos, hacer la extracción de las bases de datos y procesar transacciones fraudulentas bajo el *Shell Command* en la sección de *Meterpreter* en una conexión remota ejecutada por el programa maligno o *Malware*.

Una vez Burkov obtuvo acceso al sistema, creó una sección Backdoor para poder acceder frecuentemente al banco de data, con fin de sostener su clientela y un mercado activo. Luego de adquirir la data, Aleksei Y. Burkov procedió a liquidar la información robada por

medio de una página web bajo el dominio de Cardplanet. Este instalo un comercio digital para comprar y vender números de tarjeta de pago (débito y crédito) robadas. Además la página web ofrecía servicios de pago que permitía a los compradores comprobar si una tarjeta de pago robada aún era legítima. A continuación figura 2 muestra cómo se constituye el esquema utilizado por Burkov.

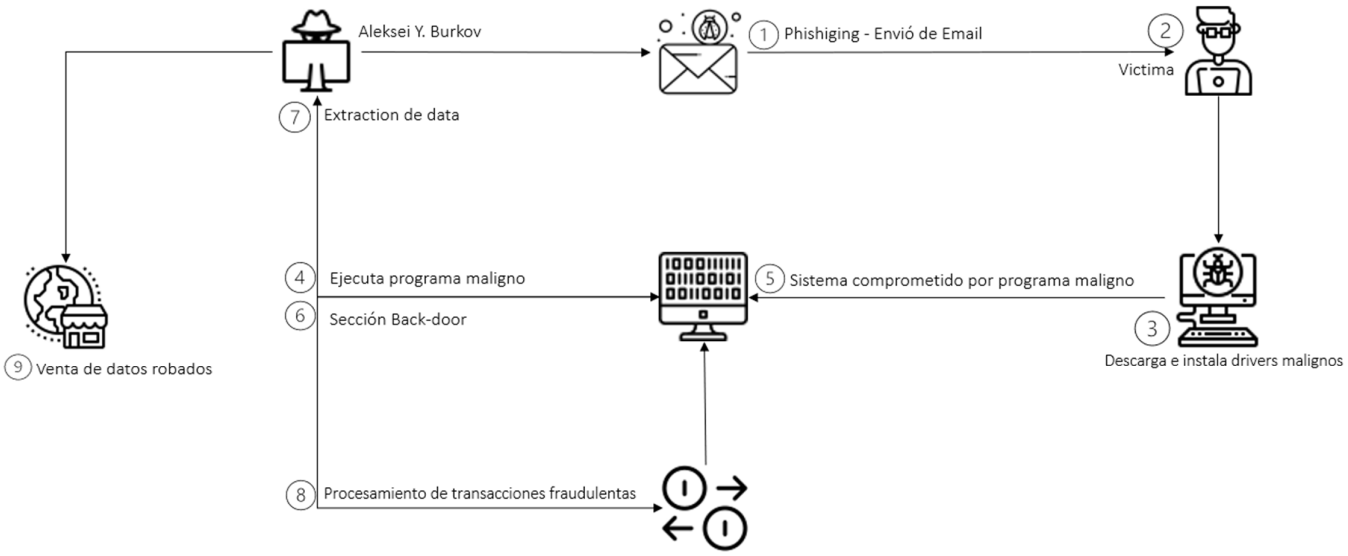


Figura 2: Esquema de fraude en el caso US. vs Aleksei Y. Burkov

INFORME FORENSE DEL CASO

Resumen Ejecutivo

Aleksei Y. Burkov es sospechoso de cometer fraude electrónico, fraude a dispositivos y conspiración para llevar acabo estos; Se le acusa de utilizar equipos electrónicos para llevar acabo un esquema de fraude basado en robo de información asociada a tarjetas de crédito e información bancaria para lucro personal por medio de un negocio en página web.

Se ha solicitado los servicios para descubrir y recuperar información electrónica ubicada en una copia entregada en una memoria USB. La evidencia entregada es una copia de la imagen del disco duro incautado al acusado. La investigación se centra en llevar acabo un análisis del disco incautado; Cabe mencionar que este dispositivo podría contener evidencia inculpatoria vital para el enjuiciamiento y convicción del acusado.

Objetivo

El objetivo de la investigación se centra en analizar, descubrir y recuperar información electrónica almacenada en una imagen del disco contenida en el USB entregado; Presuntamente relacionada con hurto de información personal, información bancaria e información de métodos de pago. El propósito de obtener posible material evidenciario que ayude a determinar los hechos probatorios.

Alcance del trabajo

En noviembre 28 del 2021 el Fiscal Federal Kellen Dwyer hizo entrega del dispositivo físico Memoria USB Marca PNY 2.0 Attaché 4, con el número de identificación USB20FD-1:15-cr-00245-TSE. El dispositivo entregado contiene una copia de la imagen del disco, propiedad del acusado. Se asegura por parte del Fiscal que entrega copia fidedigna que cumple con los estándares legales requeridos para la admisibilidad ante el juicio.

La investigación se llevará a cabo con FTK Access Data Imager; Esta herramienta se considera de estándares de excelencia en la industria de la investigación forense para la extracción de copia de la evidencia entregada por el Fiscal Federal Kellen Dwyer, para su posterior análisis. El propósito de la investigación consiste en descubrir, recuperar y preservar cualquier evidencia relevante encontrada en los registros con el propósito de ser analizada y posteriormente ser presentada como evidencia; Esto con el propósito del análisis parte del interés existente de recupera datos relevantes que sirvan como evidencia inculpatoria.

Para minimizar la posibilidad de que la evidencia se halle inadmisible se tendrá en cuenta el modelo el Electronic Data Recovery Model como referencia para así obtener una evidencia correctamente preservada, integra y confiable, convirtiéndola así en evidencia electrónica defendible jurídicamente. A continuación, un diagrama en la figura 3.

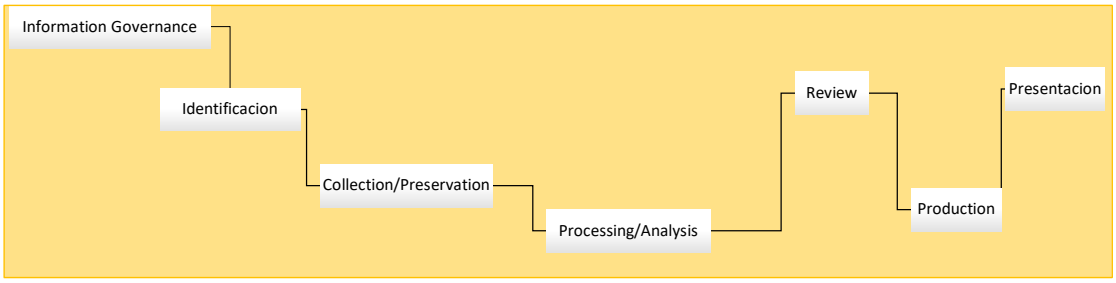


Figura 3: Diagrama del Modelo EDRM

Descripción del caso

Numero de caso: 1:15-cr-00245-TSE

Investigador: Coral N. Bautista Liz

Cliente: Fiscal Federal Kellen Dwyer

Agencia: Oficina del Fiscal de los Estados Unidos del distrito oriental de Virginia – División de Alexandria

Descripción de los dispositivos utilizados

A continuación, se detallan los dispositivos utilizados durante el proceso investigativo.

1. **Lenovo 510R-15ARR**- Donde residen todas las herramientas y aplicaciones que serán utilizadas en este proceso. A continuación la ilustración en la figura 4, sobre las especificaciones de la herramienta.

Figura 4: Especificaciones de la maquina

2. **USB 2.0 PNY Attaché 4 32GB** – Memoria en entregada por fiscalía federal con copia de los registros. A continuación las figuras 5 y 6 sobre el dispositivo provisto.

Figura 5: Memoria USB Frente

Figura 6: Memoria USB Reverso

3. **Access Data FTK-toolkit –** Herramienta con la que se desvelara la evidencia en exposición para su análisis. A continuacion una representacion visual en la figura 7.

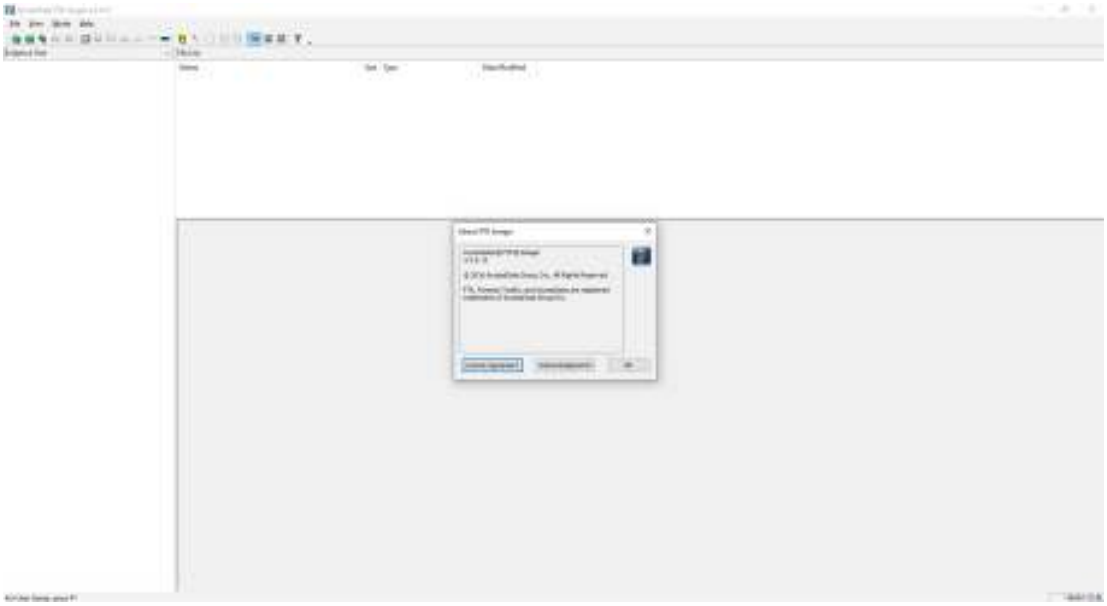


Figura 7: Especificaciones de la versión utilizada

Resumen de hallazgos

Luego de culminar el proceso de análisis del contenedor de evidencia RepositoryCapture.E01 captura realizada del USB 2.0 PNY Attaché 4 32GB, ID: USB20FD-1-15-cr-00245-TSE por medio de la herramienta FTK Imager se lograron descubrir múltiples archivos en los siguientes formatos:

- ✓ .png
- ✓ .xlsx
- ✓ .pdf
- ✓ .xls

Los archivos analizados se catalogan de dos formas:

1. Existentes: descubiertos a simple vista al observar el contenido de la imagen en FTK.
2. Borrados: archivos descubiertos luego de analizar la imagen con la opción de recuperación de archivos borrados.

A continuación se entrega a modo de muestra, una copia digital de la imagen que contiene los archivos de la evidencia exportada de la carpeta de [root] donde se localizaban los únicos registros de la captura de la memoria digital que por la naturaleza de la información contenida se catalogan como evidencia inculpatoria con relación al acusado en este caso.

[root] - copia.zip

A continuación se describirá en detalle todos los documentos hallados en la captura de la imagen utilizando FTK Image; Los archivos recuperados con FTK Image que no son visualmente reconocibles que se expondrán archivos recuperado de la extracción con FTK Image para propósito de exposición. En la figura 8 se muestra copia de un recibo con información bancaria en formato PDF.

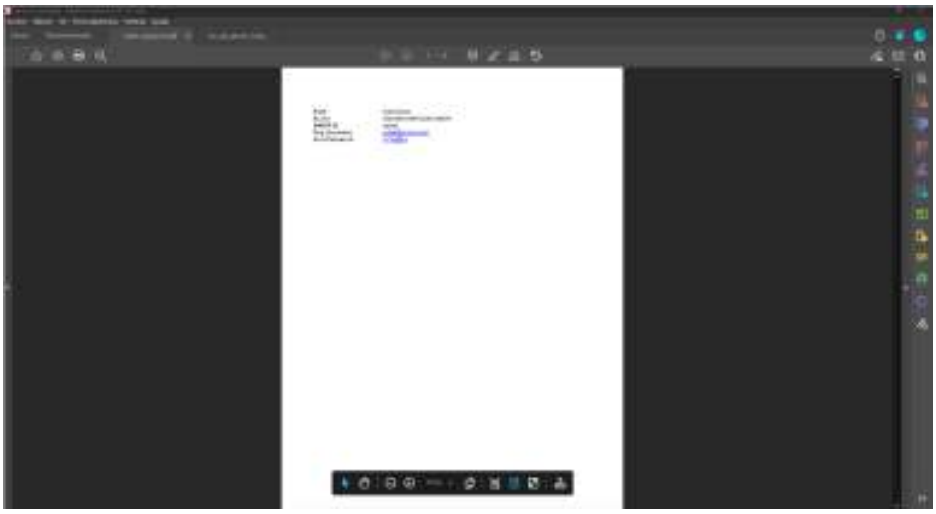


Figura 8: Copia del recibo

Al continuar revisando los archivos recuperados, se localizan varias imágenes de correos electrónico con información que vinculan al imputado con los hechos. A continuación representación visual en las figuras 9 y 10.

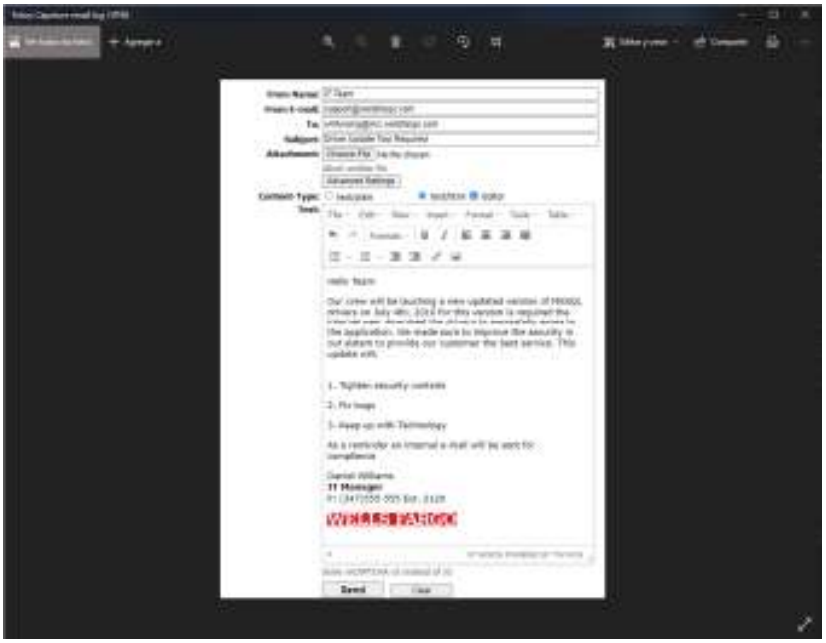


Figura 9: Primer correo electrónico enviado

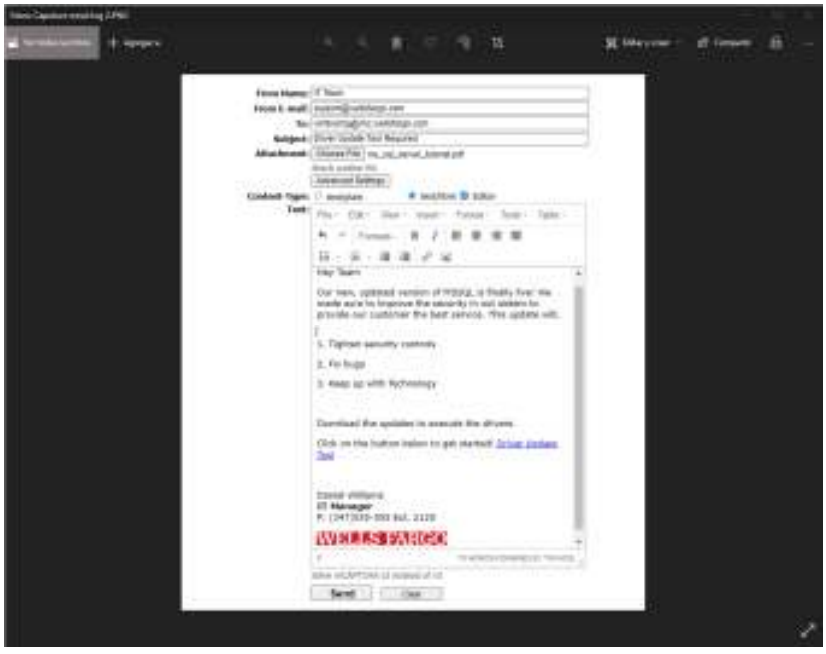


Figura 10: Segundo correo electrónico enviado

Otro de los registros localizados dentro de la carpeta de *repository*, es una lista de clientes que contiene nombres, nombres de compañías, dirección, números telefónicos y correos electrónicos. A continuación una representación visual en la figura 11.

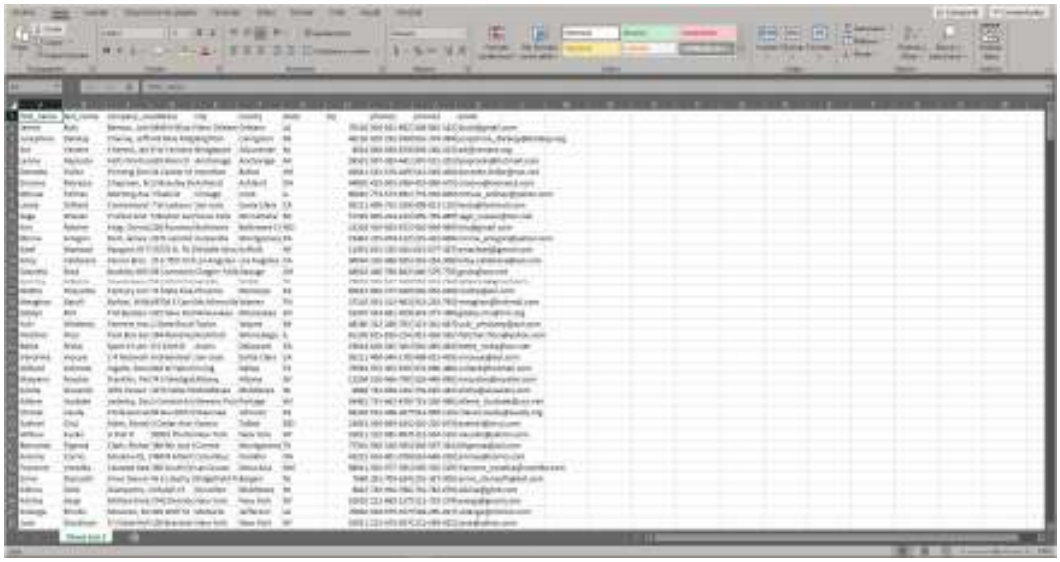


Figura 11: Lista de cliente

También se recuperó un manual PDF, se presume se utilizó el mismo para adjuntarlo al correo electrónico para hacer más creíble su táctica. A continuación una referencia visual en la figura 12.

Figura 12: Manual MSSQL

Entre otros de los registros se recuperaron 2 imágenes logotipo de un banco. Figura 13 y 14.

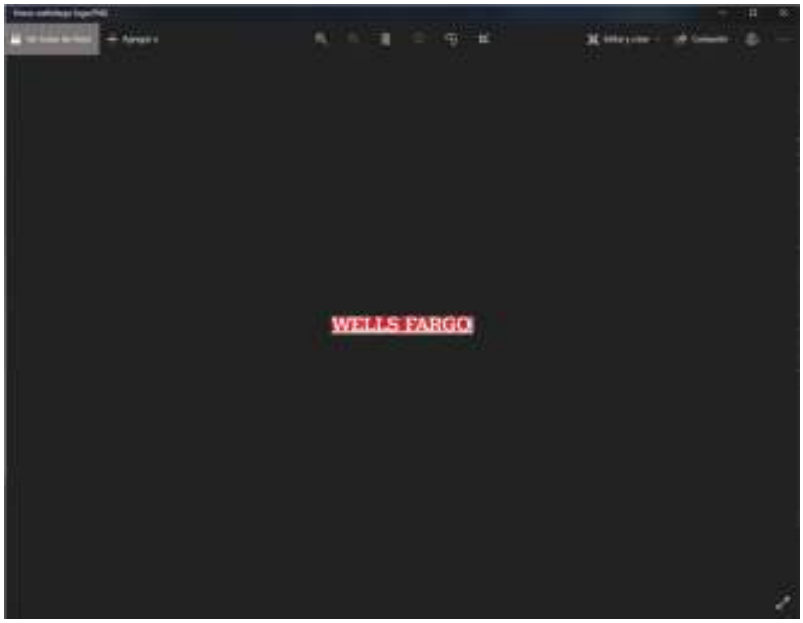


Figura 13: Logotipo del banco

Figura 14: Logotipo del banco

Para poder visualizar, aquellos documentos no legibles para propósito de la exposición se procede a exportar el reporte realizado por FTK Imager.

Entre los recuperados se encuentran 2 tablas con información de clientes, que sostienen detalles como nombres, número de tarjeta, CVV, número PIN, nombre de proveedor, numero de cuentas, correo electrónico y dirección. A continuación una representación visual en las figuras 15 y 16.

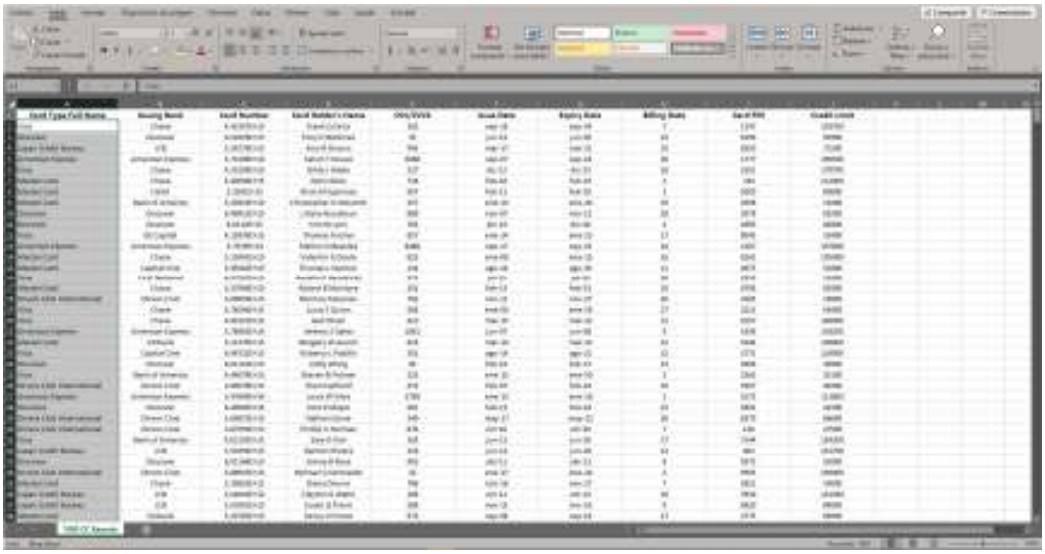


Figura 15: Lista con información de tarjetas de pago

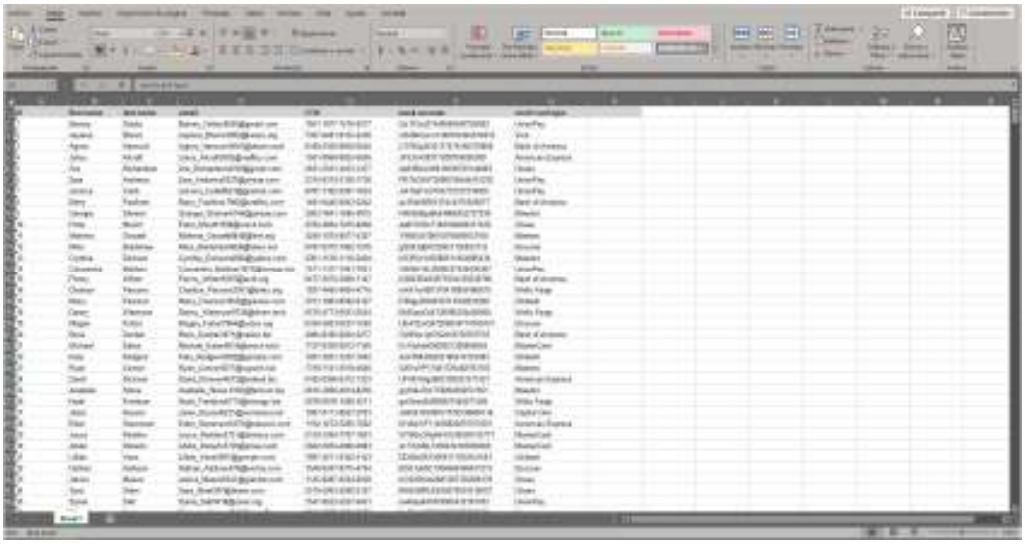


Figura 16:Lista de información de clientes y cuentas bancarias

Además de encontró copia de un estado de cuenta. A continuación una representación visual en la figura 17.

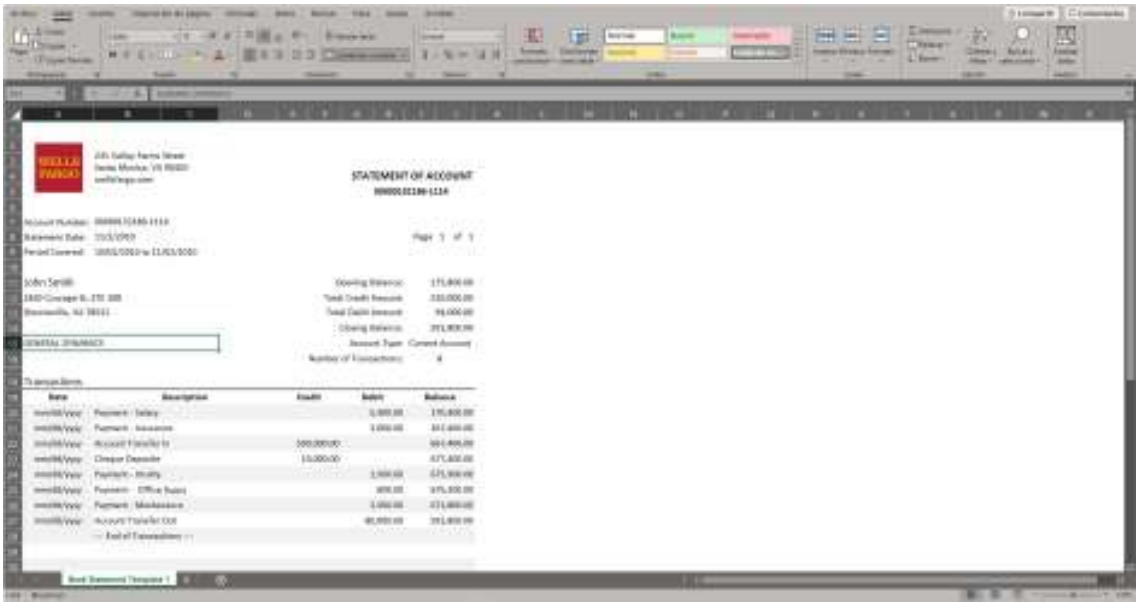


Figura 17: Estado de cuenta

Cadena de Custodia

Como parte del análisis de la prueba, se llevará a cabo el procedimiento controlado para recuperar la evidencia inculpatoria de los delito.

En el siguiente documento se detalla la cadena de custodia seguida por Coral N. Bautista Liz, investigadora designada por fiscalía federal.

Primer evento:

- **Descripción del evento:** Evidencia entregada personalmente por el Fiscal Kellen Dwyer. La evidencia entregada es una memoria USB 2.0 marca PNY modelo Attache 4 con el código de identificación USB20FD-1:15-cr-00245-TSE.
- **Evento verificado por:** Coral N. Bautista Liz, investigadora y Kellen Dwyer, Fiscal Federal

- **Entregado a:** Coral Bautista Liz, investigadora.
- **Núm. de evidencia:** USB20FD-1:15-cr-00245-TSE
- **Fecha de comienzo:** noviembre 28, 2021 – 2:00 Pm
- **Fecha de terminación:** noviembre 30, 2021 – 2:00 Am
- **Lugar de origen:** Cuarto de evidencias oficina, Coral Bautista Liz
- **Destino:** Archivero de clasificación del Fiscalía Federal

Segundo evento:

- **Descripción del evento:** Creación de número de caso y asignación de evidencia al mismo.
- **Evento verificado por:** Coral N. Bautista Liz
- **ID de evidencia:** USB20FD-1:15-cr-00245-TSE
- **Núm. del caso:** 1:15-cr-00245-TSE
- **Fecha de comienzo:** noviembre 28, 2021 – 2:00 Pm
- **Fecha de terminación:** noviembre 30, 2021 – 2:00 Am
- **Lugar de origen:** Laboratorio forense: cuarto de evidencias oficina Coral Bautista Liz
- **Destino:** Archivero de clasificación del Fiscalía Federal

Tercer evento:

- **Descripción del evento:** Proceso de adquisición de evidencia, captura de imagen de memoria, análisis de evidencia.
- **Evento verificado por:** Coral N. Bautista Liz
- **ID de evidencia:** USB20FD-1:15-cr-00245-TSE
- **Núm. del caso:** 1:15-cr-00245-TSE
- **Fecha de comienzo:** noviembre 28, 2021 – 2:00 Pm

- **Fecha de terminación:** noviembre 30, 2021 – 2:00 Am
- **Lugar de origen:** Laboratorio forense: cuarto de evidencias oficina Coral Bautista Liz
- **Destino:** Archivero de clasificación del Fiscalía Federal

Cuarto evento:

- **Descripción del evento:** Culminación del informe de análisis forense para su evaluación.
    1. Documentación de proceso investigativo y evidenciario.
    2. Informe fue entregado directamente al fiscal federal Kellen Dwyer por e l investigador a cargo de la evidencia, Coral N. Bautista Liz
    3. Devolución de la evidencia original entregada por el fiscal Kellen Dwyer.

  Nota: La evidencia original fue entregada directamente al fiscal Kellen Dwyer. por el investigador a cargo de la evidencia, Coral N. Bautista Liz.

  El análisis se repitió por última vez, 11/28/2021 como parte del proceso de revalidación de los cálculos analíticos y recopilación de evidencia.
- **ID de evidencia:** USB20FD-1:15-cr-00245-TSE
- **Núm. del caso:** 1:15-cr-00245-TSE
- **Fecha de comienzo:** noviembre 28, 2021 – 2:00 Pm
- **Fecha de terminación:** noviembre 30, 2021 – 2:00 Am
- **Lugar de origen:** Laboratorio forense: cuarto de evidencias oficina Coral Bautista Liz
- **Destino:** Archivero de clasificación del Fiscalía Federal

Procedimiento

A continuación se describirá en detalle todos los procesos realizados para examinar la evidencia las técnicas, herramientas y metodologías para extraer información significativa relacionada al caso.

Una vez completada la importación de la copia de la evidencia a FTK, se continuó expandiendo las carpetas recuperadas dentro de la memoria. A continuación una representación visual en las figuras 18 y 19.

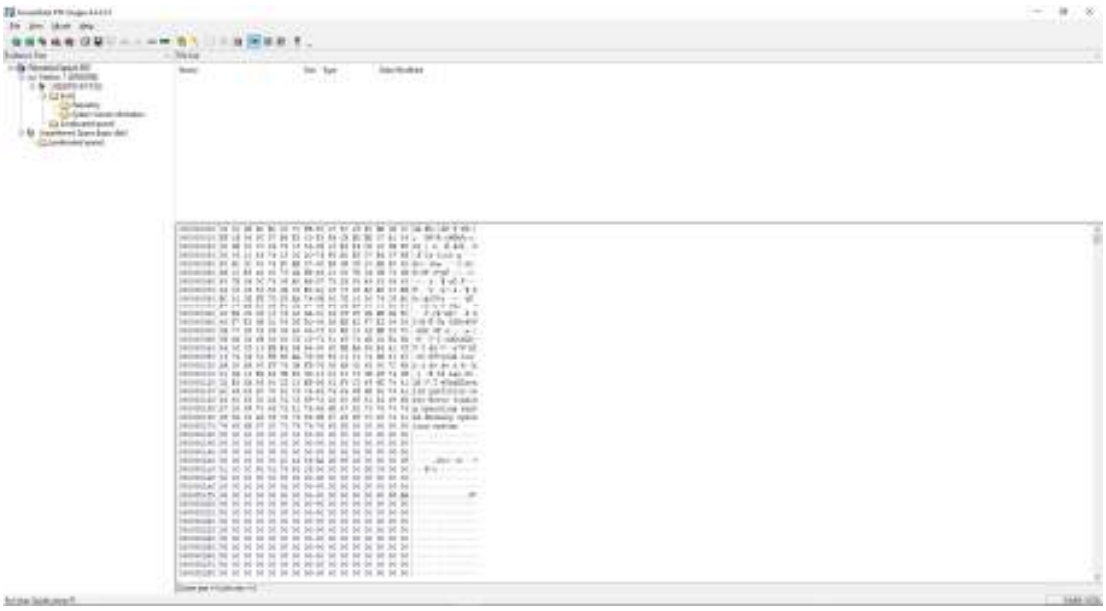


Figura 18: Visualización inicial luego de importar la imagen

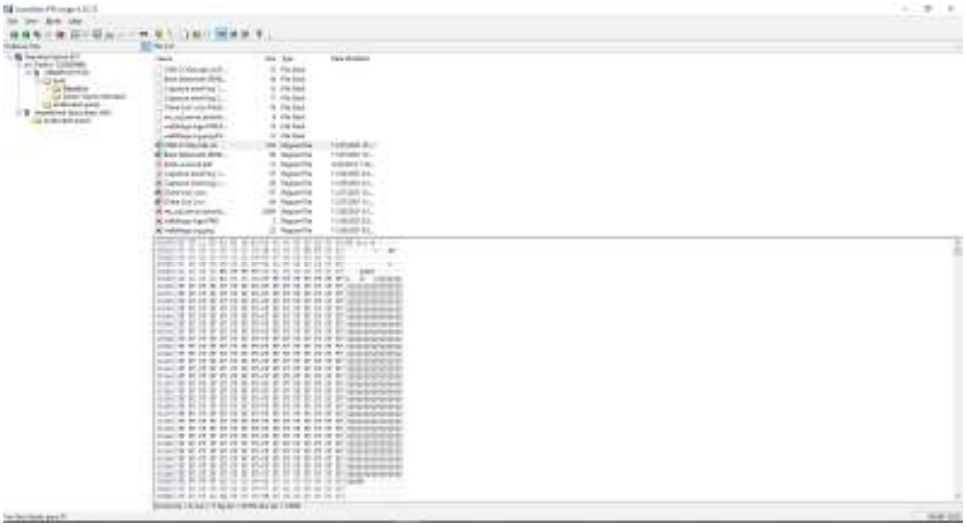


Figura 19: Registros hallados dentro de las carpetas

A continuación se describirá en detalle todos los documentos hallados en la captura de la imagen utilizando FTK Image.

Navegando entre los registros recuperado de la captura de la memoria USB 2.0 PNY Attaché 4 32GB, ID: USB20FD-1-15-cr-00245-TSE; bajo la carpeta [root] se localizan varios archivos, luego de extenderlos e ingresar a la carpeta “Repository” FTK exhibe los documentos recuperado de la extracción. En la figura 20 se muestra copia de un recibo con información bancaria en formato PDF.

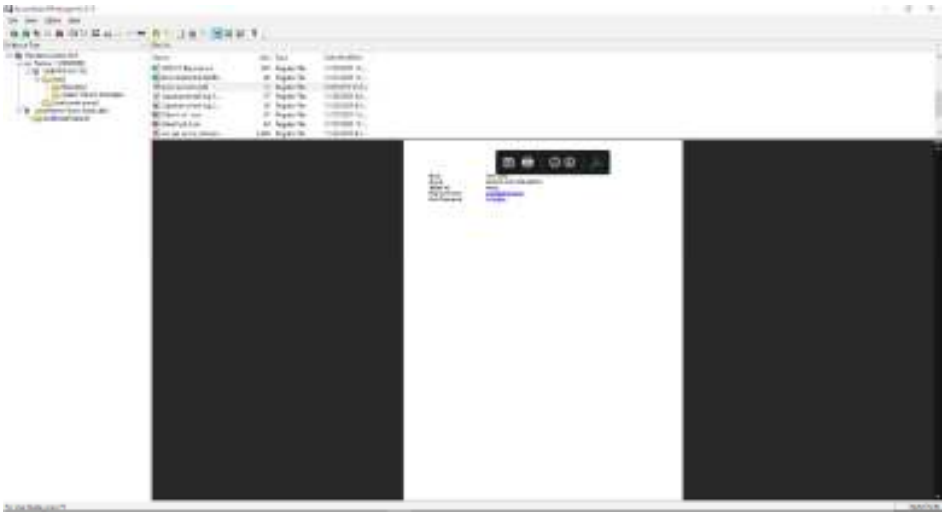


Figura 20: Copia del recibo

Al continuar revisando los archivos recuperados, se localizan varias imágenes de correos electrónico con información que vinculan al imputado con los hechos. A continuación representación visual en las figuras 21 y 22.

Figura 21: Primer correo electrónico enviado

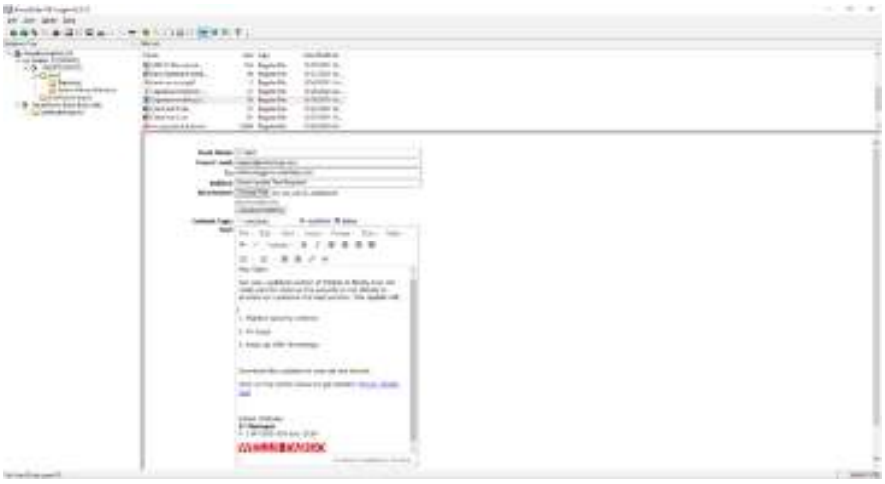


Figura 22:Segundo correo electrónico enviado

Otro de los registros localizados dentro de la carpeta de repository, es una lista de clientes que contiene nombres, nombres de compañías, dirección, números telefónicos y correos electrónicos. A continuación una representación visual en la figura 23.

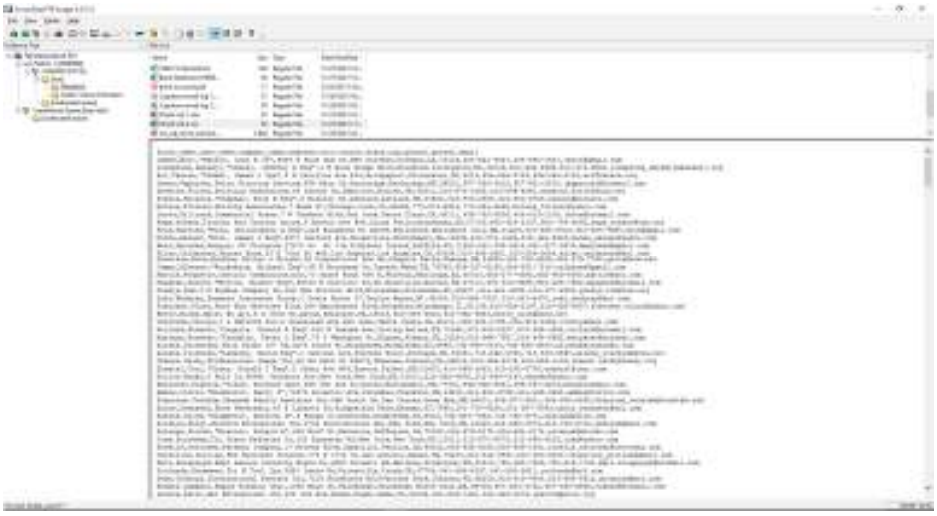


Figura 23: Lista de cliente

También se recuperó un manual PDF, se presume se utilizó el mismo para adjuntarlo al correo electrónico para hacer más creíble su táctica. A continuación una referencia visual en la figura 24.

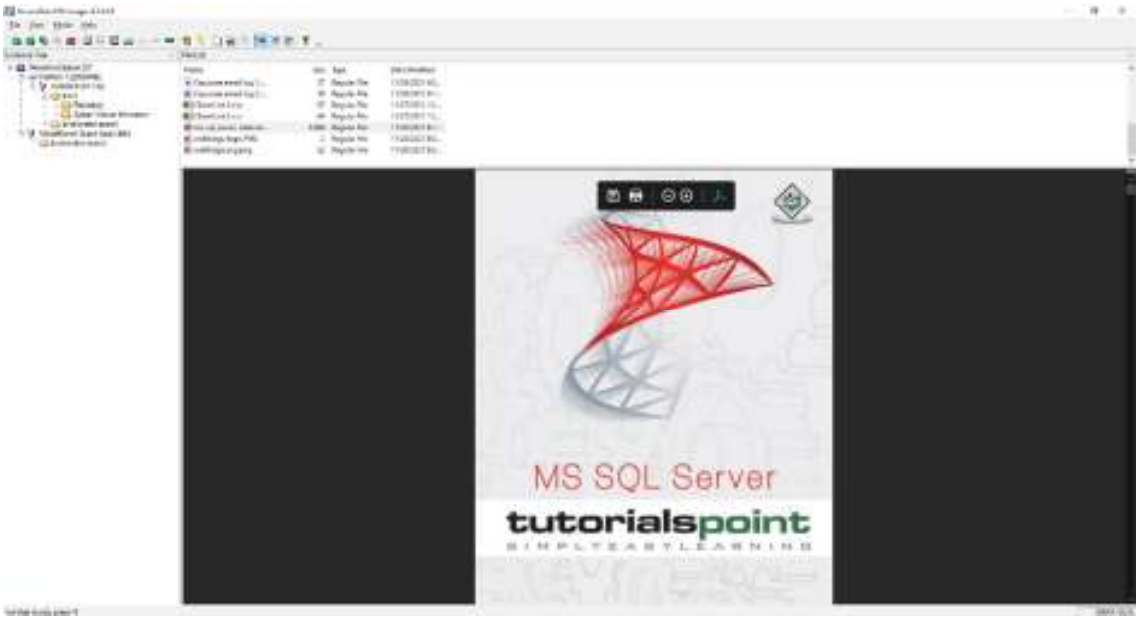


Figura 24: Manual MSSQL

Entre otros de los registros se recuperaron 2 imágenes logotipo de un banco. Figura 25 y 26.

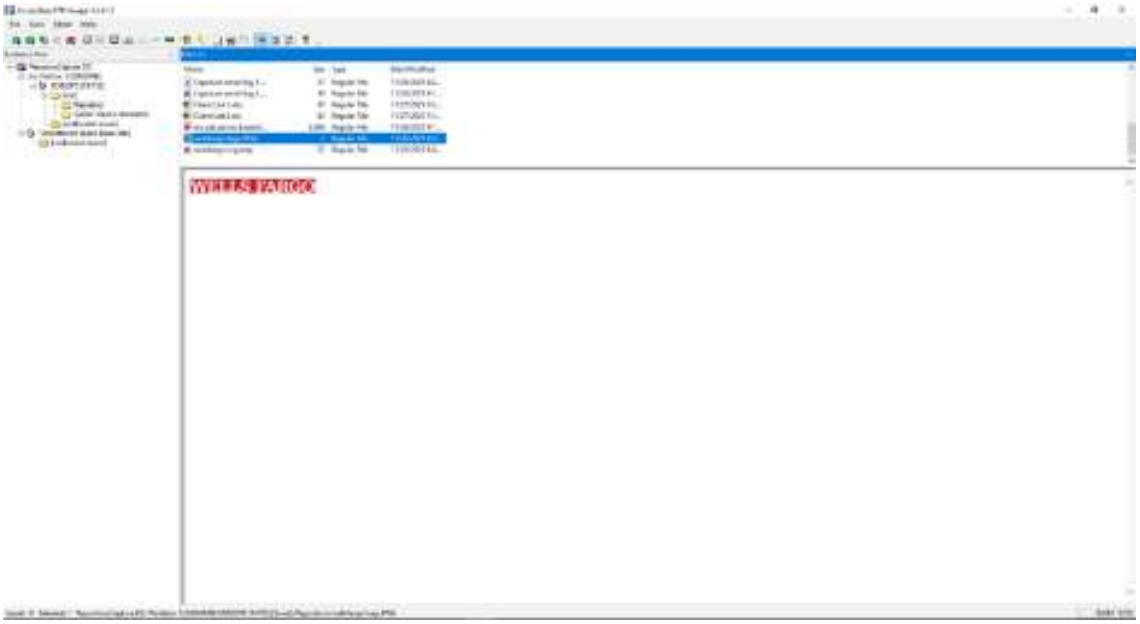


Figura 25: Logotipo del banco

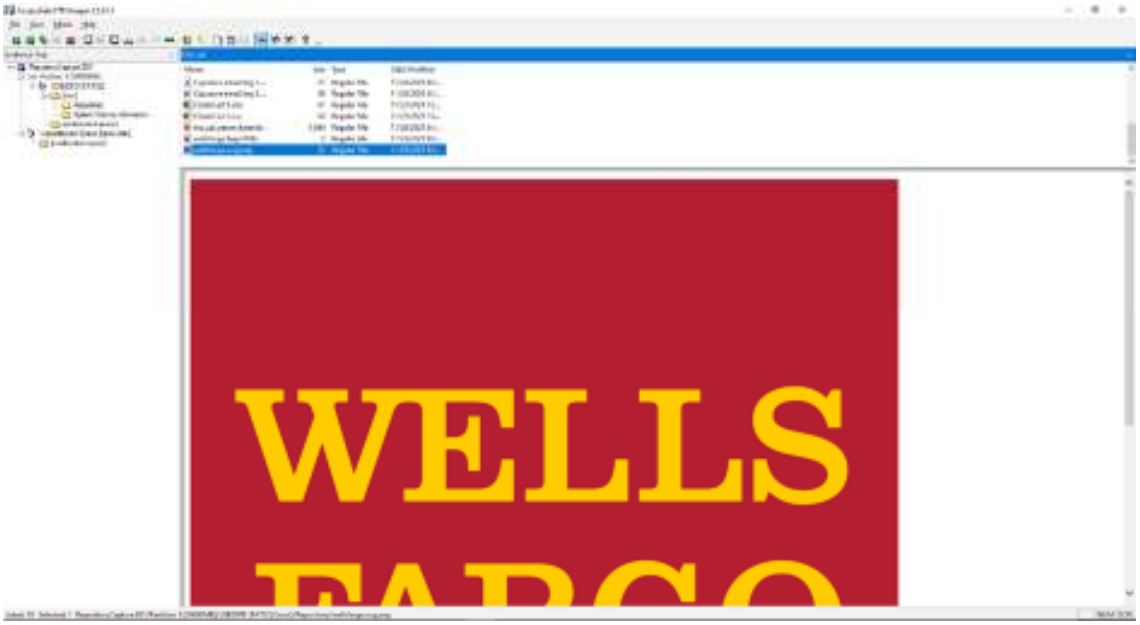


Figura 26: Logotipo del banco

Conclusión

Luego de evaluar la evidencia encontrada en la imagen analizada; Entre la evidencia identificada ante la exposición se rescataron registros de correos electrónicos, imágenes relacionada al esquema llevado a cabo, registros de información de tarjetas de pagos, y manual de majo de base datos. Además, se encontró que tenía en su posesión información confidencial como listas de clientes y transacción bancaria.

La precisión de los hallazgos apuntan al empleo de medios tecnológicos y electrónicos para la constitución de los hechos relacionado a los cargos que se le imputan al acusado. La determinación concluye así, debido a la existencia de evidencia en los equipo y servidores.

A modo de corroboración y como parte de la investigación. El análisis de la evidencia se repitió en tres (3) ocasiones para salvaguardar la integridad de la evidencia expuesta; Por lo que la información recopilada como prueba acusatoria cuanta con el aval pericial. Estableciendo que la evidencia no fue alterada por nadie al momento de la evaluación, según lo establecido en la cadena de custodia. Se concluye, 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

El caso está relacionado a delitos como, ciber-crimen, fraude financiero y robo de identidad. Este caso resalta los riesgos de la externalización de sistemas informáticos al momento de seleccionar bases de datos extranjeras como administradores informáticos. Además, exhibe el exponencial riesgo al que estamos expuestos como sociedad. La metodología empleada para sustraer la información sobre las tarjetas de crédito implicaba; instrucción informática a servidores pertenecientes de los Estados Unidos. Este colectaba copias de base de datos con la información sobre pagos, que posteriormente seria vendida en su portal web afueras de los servidores estadounidenses.

La necesidad de establecer un sistema de seguridad, adecuadamente amplio y detallado que permita salvaguardar cualquier información digitalizada, es de suma importancia; sobre todo cuando la información que se maneja es de carácter sensible. Los delitos de esta naturaleza se cataloga como, agresión contra la propiedad íntima personal, las organizaciones y el Estado.

Como investigadora, entiendo que este caso expone todos los mecanismos sobre la complejidad que implica el robo de identidad y el fraude financiero a través de técnicas como el hacking. Partiendo de la evaluación final del caso se determina, es importante establecer auditorías internas preventivas trimestrales, o según el volumen y flujo de transacciones a finalidad de detectar fallas y ausencias en los controles de las operaciones que no permitan para contrarrestar los factores de las condiciones que dan paso a situaciones igual o similares.

AUDITORIA Y PREVENCIÓN

Introducción

Desde hace varios años, el uso de la tecnología se ha vuelto una parte fundamental de la vida cotidiana, haciendo de esta un campo vulnerable en cuanto a seguridad de la información que se almacena, administra y se comparte; por lo que la administración de información de tarjetas de pago a través de internet, aun mas con el incremento masivo del comercio y banca digital. Este aumento exponencial en el uso de tarjetas de pago a través de internet trae con sigo el riesgo inherente de la comisión de fraude financiero y de robo de identidad.

Partiendo de que la información se almacenaba en servidores que comparten y administran los datos financieros de los clientes por las organizaciones, se debe emplear mecanismos robustos de seguridad para reducir los riesgos, ya que estos sistemas son vulnerables y propensos al hurto de data y fraude financiero; como se expone en el caso en estudio USA vs. Aleksei Y. Burkov (2015)

Por esto, es importante tener en cuenta los siguientes factores como indicadores de posible fraude bancario y robo de identidad:

1) Cargos excesivos en compras
2) Transacciones que no guardan relación con el cliente
3) Estados financieros que no guardan relación con el cliente
4) Cambios drásticos en las cuentas del cliente

Resumen de hallazgos

A continuación se detallan los dos hallazgos encontrados a partir del esquema llevado a cabo para la constitución de los delitos.

Primer hallazgo:

Condición: Las condiciones de la situación muestra que el empleado no fue diligente y precavido en comprobar la dirección proveniente del correo que le informaba sobre la actualización que dio paso al acceso y a cuantos más se dirigía el correo.

Criterio: El empleado de la empresa debió consultar con operaciones al recibir el correo, para asegurar los protocolos que se llevarían a cabo a partir de la actualización, ya que este contaba con acceso privilegiado al sistema.

Causa: La condición fue causada por fallas en los controles del cumplimiento normativo en la política de seguridad establecida.

Efecto: El impacto de este hallazgo se refleja en la perdida de sobre 150,000 datos de información bancaria y métodos de pagos.

Segundo hallazgo:

Condición: El sistema de transacciones no mantenía un control segregado de identificación de usuarios.

Criterio: El departamento de informática debió establecer controles de identificación segregados para cada función administrativa.

Causa: La condición fue causada por la ausencia de un control interno informáticos que exigiera un proceso de identificación según cada plataforma de función administrativa.

Efecto: El impacto de este hallazgo se refleja en la perdida de sobre 20 millones de dólares.

Opinión de Auditoria

Los efectos de las condiciones denotan la severidad de las fallas encontradas en la organización. Como parte de las recomendaciones para detectar y mitigar este tipo de vulnerabilidades cuales representan una amenaza para las instituciones financiera y los clientes se recomienda:

1) Capacitación continua a los empleados sobre las políticas de seguridad y el cumplimiento normativo para el cumplimiento correcto de los controles internos.
2) Controles de seguridad informática para evitar las descargas no autorizadas.
3) Aplicar Softwares integral de la seguridad para la detección de phishing y malwares.
4) Establecer controles de seguridad informáticos que requieran el proceso de identificación antes de ingresar a plataformas administrativas.
5) Establecer controles de rastreo en el sistema sobre las transacciones generadas por un mismo cliente.
6) Emplear herramientas de riesgos y fraudes para la empresa como el programa Decision Manager.

Es importante establecer auditorías internas preventivas trimestrales, o según el volumen y flujo de transacciones a finalidad de detectar fallas y ausencias en los controles de las operaciones diarias para contrarrestar los factores de las condiciones.

CONCLUSIÓN

Las amenazas a la seguridad en Internet se han disparado de forma alarmante en los últimos años. Tal como hemos podido comprobar por medio de una exhaustiva investigación los crímenes cibernéticos dejan un impacto severo en daños. Tomando por base el caso de estudio, los crímenes cibernéticos relacionados con el robo de identidad, por regla genérica ocurren a través de técnicas de phishing. Por otro lado emplear el uso de *malware* y hacking al ejecutar un esquema de fraude agravia la situación, ya que denota la intención maliciosa del ofensor. Este tipo de delitos representan un agresión contra la propiedad íntima personal, las organizaciones y el Estado.

Por desgracia los delitos informáticos no se pueden eliminar de manera definitiva debido al desarrollo constante de la tecnología presente hoy día, que da brecha a nuevos modos de infringir la ley, o cometer fraude. De igual forma, es importante resaltar que la cobertura legal no cobija los diversos esquemas fraudulentos que se puedan llevar a cabo, dejando una laguna entre las responsabilidades judiciales que se le puedan atribuir al infractor, contrario a los daños causados.

La necesidad de establecer un sistema de seguridad, lo suficientemente abarcador y robusto que permita salvaguardar la integridad de la información, se hace más relevante a diario; sobre todo cuando la información que se maneja es de carácter sensible, como información de identificación personal, información financiera, o detalles de organizaciones como credenciales de usuario, o documentos oficiales internos. Herramientas como regulaciones legales apoyadas en las modalidades delictivas de actualidad, ayudarían a canalizar y controlar la tasa de incidencia, de igual forma controles avanzados tecnológicos de vanguardia que vayan a la par con los criterios necesarios para prevenir, contrarrestar y restaurar daños.

REFERENCIAS

BNC. (2019). Informe. Los delitos cibernéticos en la legislación estadounidense. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf

Cornell Law School. (s. f.-a). 18 U.S. Code § 1029 - Fraud and related activity in connection with access devices. LII / Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/1029

Cornell Law School. (s. f.-b). 18 U.S. Code § 1343 - Fraud by wire, radio, or television. LII / Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/1343

Cornell Law School. (s. f.-c). 18 U.S. Code § 1349 - Attempt and conspiracy. LII / Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/1349

Department Of Justice. (2020, 26 junio). Russian National Sentenced to Prison for Operating Websites Devoted. https://www.justice.gov/opa/pr/russian-national-sentenced-prison-operating-websites-devoted-fraud-and-malicious-cyber

Federal Bureau of Investigation. (2020). Internet crime report 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Fuentes, L. (2008). Malware, una amenaza de internet. Revista Digital Universitario. http://www.revista.unam.mx/vol.9/num4/art22/art22.pdf

Móstoles, R. (2019). Acceso ilícito a sistemas informáticos. Vilches Abogados. Madrid https://blog.hernandez-vilches.com/ciberdelitos/intrusion-informatica-acceso-ilicito/

Schwartz, F., & Volz, D. (2019, 12 noviembre). Israel Extradites Accused Russian Cybercriminal to U.S. (Updated). Databreaches.Com. https://www.databreaches.net/israel-extradites-accused-russian-cybercriminal-to-u-s/

Times of Israel. (2019, 11 noviembre). Israel extradites Russian hacker to US despite Moscow's protests | The. https://www.timesofisrael.com/israel-extradites-russian-hacker-to-us-despite-protests-by-moscow/

USA vs. Alla Witte, aka Max. (1:20cr440) https://www.justice.gov/opa/press-release/file/1401766/download

USA vs. Erick Meiggs and Declan Harrington. (19cr10438) https://www.justice.gov/opa/press-release/file/1217436/download

United States v. Aleksei Burkov. (2020, 29 mayo). (115cr00245TSE) Justice.Gov. https://www.justice.gov/usao-edva/united-states-v-aleksei-burkov