EDP UNIVERSITY OF PUERTO RICO INC.
RECINTO DE HATO REY
ESCUELA GRADUADA
PROGRAMA DE MAESTRÍA EN SISTEMA DE INFORMACIÓN
Especialidad en Seguridad de Información e Investigación de Fraude

ANÁLISIS DEL CASO: COMPROMISO DE CORREO ELECTRÓNICO EMPRESARIAL (BUSINESS EMAIL COMPROMISE)

United States v Odufuye, Adejumo & Nwoke
Número de Caso: 3:16-cr-00232/3:18-cr-00082
REQUISITO PARA LA MAESTRÍA EN SISTEMA DE INFORMACIÓN
Especialidad en Seguridad de Información e Investigación de Fraude

DICIEMBRE 2018

PREPARADO POR
DINOSHKA M. VALENTÍN FLORES

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

ANÁLISIS DEL CASO: COMPROMISO DE CORREO ELECTRÓNICO EMPRESARIAL
(BUSINESS EMAIL COMPROMISE)
UNITED STATES V ODUFUYE, ADEJUMO & NWOKE
Número de caso: 3:16-cr-00232/3:18-cr-00082

Preparado por:
Dinoshka M. Valentín Flores

Ha sido aceptado como requisito parcial para el grado de:
Maestría en Sistemas de Información
Especialidad en Seguridad de Información e Investigación de Fraude

Diciembre 2018
Aprobado por

Dr. Miguel A. Drouyn, Director

TABLA DE FIGURAS

SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO

Introducción

Hoy día la tecnología se ha convertido en una parte esencial en el diario vivir del ser humano. Gracias al avance en las conexiones inalámbricas, podemos mantenernos comunicados mediante las redes sociales o realizar distintas transacciones electrónicas en nuestro diario vivir. En cierta perspectiva, es una ventaja positiva que la tecnología siga avanzando para facilitar muchas actividades al ser humano, pero visto desde otra perspectiva dichos avances pueden ser utilizados de forma negativa en manos equivocas. Dentro de esta última perspectiva se han desarrollado grandes delitos gracias al fácil acceso que los avances tecnológicos han provistos.

Hemos visto en la trayectoria de los años que ha incrementado el uso de dichos recursos de forma negativa, es decir, para crear distintas modalidades delictivas que los perpetradores cometen a la hora de realizar un acto ilícito. La facilidad con la que se realizan estos crímenes cibernéticos ha causado un gran daño a la sociedad, incluyendo tanto a individuos como a distintas empresas.

Estos crímenes pueden comenzar desde el robo de identidad, distribución de información personal, pornografía, robo de dinero en cuentas bancarias, *phishing*, entre otros tipos de fraude. Para resolver este problema es importante establecer ciertas leyes que establezcan un orden, para intentar evitar que las personas sigan cometiendo dichos delitos. Adicional, es fundamental establecer ciertas seguridades y controles en el ámbito tecnológico para evitar que los perpetradores logren el objetivo de cometer fraudes electrónicos.

Esta investigación expone un caso de fraude electrónico, el mismo se realizó por medio de correos electrónicos, siendo enviado a distintas empresas corporativas. El caso expuesto será

Estados Unidos V. Lumuyiwa Yahtrip Adejumo y Odufuye. Los perpetradores mediante correos electrónicos se hacían pasar por el Principal Oficial Ejecutivo (CEO por sus siglas en inglés) de la empresa, y en dicho correo exigían un depósito a una cuenta ajena a la empresa; con este esquema lograron defraudar a la compañía por millones de dólares. En la investigación se observará las decisiones legales que se le imputaron a los delincuentes.

El propósito de esta investigación es educar a las personas para que no sean víctimas de este fraude electrónico que se presenta y prevenir que esta modalidad siga expandiéndose en nuestra sociedad. En fin, es importante que a medida que la tecnología siga evolucionando, nuestra seguridad, control y organización se incremente aún más para evitar que tales actos ilícitos sean cometidos.

Descripción del caso

Número de caso

- United States v. Odufuye (3:16-cr-00232)
- United States v. Adejumo (3:18-cr-00082)

Autores y Conspiradores

- Adeyemi Odufuye
- Olumuyiwa Yahtrip Adejumo (conspirador)
- Stanley Hugochukwu Nwoke (conspirador)

Investigadores

- Patricia M. Ferrick- Agente especial de la División del FBI en New Heaven, Connecticut
- Jennifer Boyer, Agente especial del FBI
- Connecticut Cyber Task Force

Abogado

- Tracy Frederick, Defensor Federal, Distrito de Connecticut
- Robert J. Sullivan Jr, Abogado del Estado, Distrito de Connecticut

Fiscal

- John H. Durham, Fiscal de los Estados Unidos para el Distrito de Connecticut
- David T. Huang, Asistente Fiscal de los Estados Unidos

Juez

- Janet C. Hall, Jueza del Tribunal de Distrito de Connecticut

Trasfondo

Esta investigación se dirige al delito electrónico realizado por medio de correos electrónicos fraudulentos a distintas empresas corporativas. Entre los acusados se encuentran Adeyemi Odufuye conspirando con Stanley Hugochukwu y Olumuyiwa Yahtrip Adejumo. Los acusados son ciudadanos nigerianos.

Odufuye, según United States Departament of Justice (2018a), es también conocido como Micky, Micky Bricks, Yemi, GMB, Bawz y Jefe, de 32 años, residente de Sheffield, Reino Unido. Fue estudiante en la Universidad de Sheffield Hallam, graduado de una Maestría en Ciencias de Sistema de Información en Seguridad. Stanley Hugochukwu Nwoke conocido como Stanley Banks, Hugo Banks, Banks, Banky, Jose Calderon, estudio en ApTech Computer Education en Lagos, Nigeria. El otro acusado Olumuyiwa Yahtrip Adejumo se conocía también como Ade, Slimwaco, Waco, Waco Jamon, Hade y Hadey de 33 años, residente de Toledo, Ohio.

Los acusados utilizaron técnicas cibernéticas sofisticadas para estafar a las empresas. Adejumo y sus conspiradores enviaban correos electrónicos dirigidos a ejecutivos que parecían haber sido enviadas desde una dirección de correo electrónico legítima del CEO u otro ejecutivo de la empresa. Adejumo y los conspiradores enviaron los correos electrónicos con la intención de que los destinatarios enviaran o transfirieran dinero a las cuentas bancarias utilizadas por los miembros de la conspiración. El Departamento de Justicia, destaca que el FBI identificó desde septiembre de 2015 a mayo de 2016, 36 confirmaciones bancarias en las cuentas de correo electrónico que Odufuye utilizó con más de $1.6 millones en fraude. El 19 de diciembre de 2016 fue arrestado en el Reino Unido y fue extraditado de Reino Unido a Estados Unidos.

Descripción de los hechos

Basado en la investigación de los casos USA v Adejumo (2018) y USA v Odufuye (2018), desde aproximadamente el 19 de julio de 2015 y hasta el 24 de junio de 2016, Nwoke, Odufuye, Adejumo y otros conspiraron en un plan para defraudar empresas y entidades víctimas en todo Estados Unidos asumiendo falsamente la identidad de CEOs, CFOs y otros ejecutivos de las empresas y entidades víctimas para inducir a las mismas a transferir dinero a cuentas bancarias utilizadas en conspiración.

En este caso, Nwoke y sus conspiradores perpetuaron el plan para estafar a una víctima corporativa, Victim Company 1, un fabricante que tiene oficinas ubicadas en Connecticut. También a una víctima corporativa adicional, Victim Company 2, una empresa de productos industriales que tiene oficinas en Connecticut.

El individuo A es el Director Ejecutivo de la víctima 1 de la compañía, que esta fuera de los Estados Unidos. El individuo B es el controlador de la víctima 1 de la compañía. El individuo

B su responsabilidad es controlar las finanzas en la empresa. La oficina del individuo B se encuentra en Connecticut.

Usando varias cuentas de correo electrónico como se explica más adelante, Nwoke, Odufuye, y otros enviaron, o causaron que se enviaran, docenas de correos electrónicos a Individual B desde el 2 de noviembre de 2015 hasta el 10 de diciembre de 2015. En esos correos electrónicos, Odufuye y sus conspiradores se hicieron pasar por Individuo A, CEO de Victim Company 1, con el propósito que el Individuo B realizara transferencias bancarias múltiples, las cuales excedieron un total de $ 1,000,000 de las cuentas de Victim Company 1 a diversos individuos y entidades.

Alrededor del 2 de noviembre de 2015, el individuo B comenzó a recibir correos electrónicos dirigidos a él en la cuenta de correo electrónico de su trabajo que pretendía ser del individuo A. En realidad, estos correos electrónicos eran falsificado, es decir, se hizo parecer que venía del correo electrónico comercial del individuo A, cuando de hecho fueron enviados por Nwoke, Odufuye y sus conspiradores. El 2 de noviembre de 2015, se envió un correo electrónico a la Persona B que parece ser del correo electrónico del individuo A en [Individual A] @ [Victim Company l] .com. la línea del asunto decía:

"Treat this morning." ". El cuerpo del mensaje lee:

[Individuo B],

I need you to arrange a wre transfer and process it this morning.

Let mew know as soon as you see this email so I can provide you with the

banking instructions and the receiver's details, etc.

Any prior documentations will be presented later.

Thanks,

[Individuo A]

Sent from my iPhone

Un análisis más detallado de este correo electrónico reveló que, de hecho, fue falsificado y no en realidad enviado desde [Individual A] @ [Victim Company l].com. Más bien, el encabezado del correo electrónico reveló que el "X-Sender", la parte del encabezado que proporciona información sobre dónde se encuentra el correo electrónico que se originó, fue halloween@veteranboats.org y la dirección "Responder a", que es la dirección a la que se dirige un correo electrónico si el destinatario envía una respuesta, fue ceo.exeuctiveOOO@gmail.com. Los miembros de la conspiración controlaron o utilizaron tanto halloween@veteranboats.org como el ceo.exeuctiveOOO@gmail.com.

Como resultado de estos correos electrónicos fraudulentos que el individuo B creía ser legítimo y de la persona A real, Victim Company 1 envió cinco transferencias bancarias por un total de más de $500,000 de las cuentas de la compañía en Connecticut a personas desconocidas o cuentas de entidades en Hong Kong, Texas, Florida y Washington, DC. Ninguno de estas transferencias eran autorizadas o iniciadas por la persona real A o por el negocio legítimo de Victim Company 1.

Entre el 2 de noviembre de 2015 y el 9 de noviembre de 2015, el Individual B transfirió o intento transferir más de $300,000 de las cuentas de Victim Company 1 como resultado de los correos electrónicos enviado por Nwoke y sus conspiradores. El 9 de noviembre de 2015, Individuo B envió una transferencia de un monto de $188,575 para una entidad de la Entidad 1. de Hong Kong. Unos días después, el 12 de noviembre, 2015, Odufuye haciéndose pasar por el verdadero individuo A hizo la siguiente solicitud para Individuo B vía correo electrónico:

> "I will need you to arrange a second swift transfer to [Hong Kong Entity 1] for $221,430. Same banking information as well as payment reference/reason for payment. The first transfer was an initial installment. I will require copies of the confirmation accordingly when complete. Thank you."

El X-Sender para este mensaje fue de ceolevel2@veteranboats.org y la dirección de respuesta era ceo.executiveOOO@gmail.com, ambos controlados o utilizados por Nwoke u otros miembros de la conspiración. Basado en este correo electrónico, el individuo B envió esa transferencia ese día según se informó a Individuo A que enviaría la confirmación cuando la recibiera. El individuo B envió al Individuo A un archivo adjunto titulado "[Hong Kong Entity 1] Wire. pdf." El adjunto contenía una imagen del formulario de autorización de transferencia bancaria de Victim Company 1 por los $ 221,430 transferidos a la Entidad 1 de Hong Kong.

Nwoke y sus co-conspiradores también apuntaron a otra víctima corporativa, Victim Company 2. Los individuos C y D son dos de los tres dueños de la Compañía 2. Individuo E es el Director Financiero de Victim Company 2. El 2 de noviembre de 2015, Nwoke y sus

conspiradores enviaron un correo electrónico al individuo E, el cual parecía provenir del correo electrónico legítimo del individuo C en Company Victim 2.

La línea del asunto decía:

"Treat this morning."

El cuerpo del mensaje lee:

[Individual E],

I need you to arrange a wre transfer and process it this morning.

Let mew know as soon as you see this email so I can provide you with the banking

instructions and the receiver's details, etc.

Any prior documentations will be presented later.

Thanks,

[Individual C]

Sent from my iPhone

Las autoridades policiales investigaron este correo electrónico y determinaron que fue falsificado y no se envió realmente desde el correo electrónico de la persona C a la empresa de víctimas 2. Más bien, el encabezado del correo electrónico reveló que el X-Sender era halloween@veteranboats.org y que la dirección de respuesta era ceo.exeuctiveOOO@grnail.com.

El individuo E respondió:

> "Ok no problem- give me the swift and amount." Although there were additional e-mails exchanged between Individual E and the person that purported to be Individual C, Individual E did not send any money as directed.

El 10 de diciembre de 2015, Nwoke y sus conspiradores enviaron al individuo E un correo electrónico haciéndose pasar por el Individuo D, [Individual D] @ [Víctima Empresa 2].com, el correo electrónico contenía dos anexos, que Individuo E abrió.

Alrededor del 21 de junio de 2016, Individuo E recibió un correo electrónico del individuo C de la víctima 2 de la compañía con el asunto "PMTDistribution."

El texto decía:

> [Individual E],
>
> Please find attached instructions for payment of $55,375. I need this arranged to the vendor today. Let me know if you need anything in addition.
>
> Thanks,
>
> [Individual C]

Se adjuntaron en este correo electrónico instrucciones de transferencias para una cuenta en Miami, Florida. La investigación de este correo electrónico reveló que fue falsificado y en realidad no se envió desde Correo electrónico de la persona C de Victim Company 2. El

encabezado del correo electrónico reveló que el remitente X fue sonia@secondtow.info y la dirección de respuesta fue ceo.exeuctiveOOO@gmail.com.

Algunos de los correos electrónicos que los perpetradores utilizaron fueron: frank_cole8@yahoo.com, calderon.jo449@gmail.com, ceo.executiveOOO@gmail.com, ceo.exeuctiveOOO@gmail.com, praxes123@gmail.com y angelmicky_g4l@yahoo.com.

En diciembre de 2016, un gran jurado devolvió una acusación acusando a Nwoke y Odufuye en Estados Unidos v. Adeyemi Odufuye y Stanley Hugochukwu Nwoke. (Caso No. 3: 16CR232) Odufuye se declaró culpable de ciertos cargos de la acusación y espera sentencia, mientras que Nwoke espera juicio. En abril de 2018, Adejumo renunció a su derecho a la acusación, se comprometió culpable de una información, y fue sentenciado.

Acusasiones, cargos y penalidades

Dentro de las acusaciones que le sometieron a los imputados fueron las siguientes:

- Fraude Electrónico (18 USC § 1343)- Se le acusa por este delito debido al fraude que cometieron, enviando correos electrónicos solicitando dinero con la intención de utilizarlos ya sea para uso propio o un tercero en violación de la ley, utilizando la tecnología como medio primario en su acto delictivo.
- Robo de identidad agravado (18 USC § 1028)- Se le acusa por este cargo debido a que los individuos mantenían una falsa representación, haciéndose pasar por el CEO de la compañía para defraudar por un medio electrónico a las empresas.
- Intento y Conspiración (18 USC § 1349)- este delito es sometido debido a que todos los autores y conspiradores colaboraron para la comisión del delito realizado. Todos

estuvieron bajo comunicación para desarrollar el marco delictivo de este caso, con el propósito de adquirir un beneficio monetario por tal acto.

- Restitución (18 USC § 2264)- dentro de esta sección se le impone al victimario pagar a la víctima el monto total de perdidas en el que incurrieron según el tribunal lo disponga.

Olumuyiwa Yahtrip Adejumo fue sentenciado a 15 meses de cárcel seguido de tres años de libertad supervisada por los cargos de fraude electrónico y conspiración. La jueza Hall le ordenó a Adejumo que pagara una indemnización de $90,930. Por otro lado, Odufuye fue sentenciado a 45 meses de prisión por su rol de supervisor en un esquema de compromiso de correo electrónico empresarial por los cargos de conspiración para cometer fraude electrónico y un cargo de robo de identidad agravado. La jueza Hall le ordenó a Odufuye que pagara una indemnización de $921,497.87 a 15 víctimas del esquema. El otro acusado Nwoke aún está en espera de juicio.

Definiciones de términos

Fraude- según la Asociación de Examinadores de Fraude en Puerto Rico significa cualquier delito con fines de lucro que utilice el engaño como su principal modus operandis o cualquier acto intencional o deliberado para privar a otra persona de propiedad o dinero por engaño u otro medio injusto (Association of Certified Fraud Examiners, 2018b).

Fraude Electrónico- es similar a un fraude habitual, excepto que se produce a través de líneas telefónicas o implica comunicaciones electrónicas (Find Law, 2018).

Posee cuatro elementos:

1.El acusado creo o participo en un plan para estafas a otro si dinero;

2. El acusado lo hizo con la intención de defraudar;

3. Era razonablemente previsible que el demandado usara comunicaciones por cable;

4. El acusado, de hecho, utilizó comunicaciones por cable interestatal.

Business E-Mail Compromise Scheme- es un tipo de estafa dirigida a empresas que realizan transferencias bancarias y tienen proveedores en el extranjero. Las cuentas de correo electrónico corporativas o disponibles públicamente de ejecutivos o empleados de alto nivel relacionados con el financiamiento o involucrados en pagos por transferencia bancaria se falsifican o se comprometen a través de keyloggers o ataques de phishing para realizar transferencias fraudulentas, lo que genera cientos de miles de dólares en perdida (Federal Bureau of Investigation, 2018).

SECCIÓN 2: REVISIÓN DE LA LITERATURA

Introducción

En nuestra actualidad la tecnología se ha desarrollado grandemente y ha obtenido un impacto importante en nuestras vidas. La utilización de esta se ha visto del lado positivo y negativo. Por el lado negativo, notamos como los perpetradores la han utilizado para beneficiarse de algún bien común para su persona o la de un tercero, perjudicando tanto individuos como distintas empresas y/o corporaciones.

Por medio de los años las modalidades de cometer fraudes a través del Internet se han visto comúnmente debido a estos grandes cambios. Hoy día la modalidad de cometer fraudes por medio de correos electrónicos ha obtenido un alza en nuestra sociedad. Este esquema es conocido en la actualidad por Business Email Compromise por sus siglas en inglés BEC, la cual es una amenaza cibernética que se ha desarrollado en los pasados años causando una gran pérdida a distintas empresas en el mundo.

En el 2013 empezaron a rastrear estas amenazas cibernéticas financieras cuando los grupos del crimen organizado se han dirigido a grandes y pequeñas empresas y organizaciones en todos los estados de USA (United States of America) y en más de 100 países de todo el mundo. Las pérdidas son sobre más de miles de millones de dólares. BEC se basa en el truco más antiguo del manual del estafador, el engaño (FBI, 2017).

En la mayoría de los casos, los estafadores atacan a los empleados con acceso a las finanzas de la compañía y los engañan para que realicen transferencias monetarias a cuentas bancarias que se cree que pertenecen a socios de confianza, excepto que el dinero termina en

cuentas controladas por los delincuentes. Esas técnicas incluyen tácticas en línea como *phishing*, ingeniería social, robo de identidad, *spoofing* y el uso de *malware*. Los perpetradores son tan practicados en su oficio que el engaño a menudo es difícil de descubrir hasta que es demasiado tarde. El esquema más utilizado involucra al grupo criminal que obtiene acceso a la red de una compañía a través de un ataque de *phishing* y el uso de *malware*. Mediante este método pueden pasar días o semanas sin ser detectados obteniendo información relacionada de la empresa la cual desean atacar.

Según el Centro de Quejas de Delitos por Internet del FBI, desde enero de 2015, ha habido un aumento del 1,300 por ciento en las pérdidas expuestas identificadas, que ahora suman más de $3 mil millones. Según los datos financieros que IC3 reportó, los bancos asiáticos ubicados en China y Hong Kong siguen siendo los principales destinos de los fondos fraudulentos. Sin embargo, las instituciones financieras en el Reino Unido, México y Turquía también se han identificado recientemente como destinos destacados. (Federal Bureau of Investigation, 2018)

Esta modalidad al ser tan reciente hace que las personas no conozcan al respecto de esta y a la vez sean engañados por la mentira envuelta en el delito. El esquema de Business Email Compromise continuará siendo uno de los ataques más populares, especialmente para los que carecen de herramientas y conocimientos especiales para lograr esquemas más complicados.

Por lo general, los ataques BEC no requieren herramientas complicadas ni conocimientos altamente técnicos para que un perpetrador los realice. Por tal razón es de importancia que los empleados de las empresas estén capacitados para lidiar con este esquema

que ha surgido en nuestro presente. Dado a que los ataques se están realizando con más frecuencia en distintas empresas a nivel mundial, todo el personal debería ser orientado acerca de cómo mitigar el esquema previsto y utilizar herramientas que les ayuden a detectar las claves precisas para no ser víctimas de este delito.

Fraudes Involucrados

En la mayoría de los casos bajo este esquema los fraudes mayormente involucrados son:

1. El fraude electrónico también conocido como Wire Fraud en inglés.
2. Robo de identidad

Por medio de la tecnología y/o aparatos electrónicos son cometidos estos fraudes. La manera que se van desarrollando los mismos es como logramos obtener los fraudes que se desarrollan con cada uno de los esquemas. Según Trend Micro (2016), en la situación del *Business Email Compromise* los fraudes se realizan a través de un perpetrador realizando una falsa representación de su persona para iniciar este fraude. Utilizan distintas metodologías para cometer el delito tales como: *spoofing*, *phishing* y *malwares.* Con esta base es como los investigadores llegan a concluir los fraudes que se le pueden someter a la hora de enjuiciarlos.

El fraude de robo de identidad se origina en el momento en que los estafadores se identifican a sí mismos como ejecutivos de alto nivel (CFO, CEO, CTO, etc.), abogados u otros tipos de representantes legales y pretenden manejar asuntos confidenciales o sensibles al tiempo e iniciar una transferencia bancaria a una cuenta que controlan. En algunos casos, la solicitud fraudulenta de transferencia bancaria se envía directamente a la institución financiera con instrucciones para enviar fondos urgentemente a un banco (Trend Micro, 2016).

Un estudio realizado por Javelin demuestra que el 31.7% de las víctimas de violaciones en 2016 experimentaron un fraude de identidad, en comparación con solo el 2.8% de las personas que no fueron notificadas de una violación de datos en el año 2016. El robo de identidad es uno de los resultados más comunes de las violaciones de datos (citado por Tatham, 2018).

En una encuesta que realizó Experian, a partir de agosto de 2017, a la mayoría de los estadounidenses les preocupaba que su información pudiera ser robada, ya que el 73% dijo que estaba preocupado de que su correo electrónico, cuentas financieras o información de redes sociales pudieran ser pirateados, en comparación con 69% en una encuesta similar realizada en el año 2015 (citado por Tatham, 2018).

Tatham (2018) señala que el Centro de Recursos contra el Robo de Identidad (ITRC, por sus siglas en inglés) anunció en un informe del 2017, el año pasado hubo 1,579 violaciones de datos que expusieron casi 179 millones de registros representado un aumento de 44% en el numero de violaciones y un aumento del 389% en los registros expuestos. Por otro lado, el informe también indico que la cantidad de tarjetas de crédito expuesta en el 2017 ascendió a 14.3 millones, un 88% mas que el 2016. Además, en el 2017 se expusieron cerca de 158 millones de números de Seguro Social.

Algunos tipos de robo de identidad son:

1. Fraude por tarjetas de crédito es la forma común de robo de identidad con 133,015 informes reportados.
2. Fraude laboral o relacionado a impuestos con 82,051 informes reportados.

3. Fraude telefónico o de servicios públicos con 58,045 informes reportados.
4. Fraude bancario con 50,517 informes reportados.
5. Fraude de préstamos o arrendamiento con 30,034 informes reportados.
6. Fraude en documentos gubernamentales o fraude de beneficios con 25, 849 informes reportados.

Los consumidores reportaron según Tatham (2018), $905 millones en pérdidas totales por fraude en el año 2017, con un aumento del 21.6% en comparación con el año 2016. La pérdida promedio fue de $429. El 21% de los consumidores que reportaron una queja relacionada con un fraude perdió dinero. El método más común que se pagó con dinero fue mediante transferencia bancaria. El 64% de todas las quejas relacionadas con fraude informaron el método de contacto inicial. De esas quejas, el 69.8% por teléfono y el 9.7% por correo electrónico. Solo el 5% de los consumidores reportaron el correo como el punto inicial de contacto.

Entre los grupos de edad en riesgo cuando se trata de estafas, los niños y las personas mayores están en mayor riesgo. En 2017, hubo 13,852 quejas de robo de identidad de niños y adolescentes. Por otro lado, Michigan es el estado con la tasa per cápita más alta de denuncias de robo de identidad informadas. Florida, California, Maryland y Nevada completaron los 5 estados principales donde se realizaron denuncias de robo de identidad (citado por Tatham, 2018).

De acuerdo con Tatham (2018) el robo de identidad tiene consecuencias que van más allá de la pérdida de datos e información personal, ya que puede llevar mucho tiempo y dinero resolverlos y puede generar angustia emocional. El 26% de los encuestados tuvo que pedir dinero prestado a familiares o amigos. El 22% se tomó un tiempo fuera del trabajo. El 15.3% de

los encuestados vendieron posesiones para pagar los gastos causados por su robo de identidad y el 6.7% obtuvo un préstamo de día de pago.

También existe la estafa de impostores la cual comienza cuando un estafador pretende ser alguien que conoce y en quien confían. Tatham (2018) indica que cada cinco personas que fueron víctimas de una estafa de impostores perdieron dinero, por un total de $328 millones.

Leyes aplicables

- *18 U.S.C. Sección 1343 Fraude por cable, radio o televisión.*

  Quienquiera que haya ideado o tenga la intención de diseñar algún plan o artificio para defraudar, o para obtener dinero o bienes por medio de pretensiones, representaciones o promesas falsas o fraudulentas, transmita o haga que se transmita mediante comunicación por cable, radio o televisión. En el comercio interestatal o extranjero, cualquier escrito, rótulo, señal, imagen o sonido con el propósito de ejecutar dicho esquema o artificio, deberá ser multado bajo este título o encarcelado por no más de 20 años, o ambos. Si la violación ocurre en relación con, o involucra cualquier beneficio autorizado, transportado, transmitido, desembolsado o pagado en relación con, un desastre o emergencia mayor declarado por el presidente (según se definen dichos términos en la sección 102 de Robert T. Stafford). La Ley de Asistencia de Emergencia y Ayuda por Desastres (42 USC 5122), o afecta a una institución financiera, dicha persona debe ser multada por no más de $ 1,000,000 o encarcelada por no más de 30 años, o ambos.

- *18 U.S.C. Sección 1349- Intento y Conspiración*

  Cualquier persona que intente o conspire para cometer un delito en virtud de este capítulo estará sujeta a las mismas sanciones que las prescritas para el delito, cuya comisión fue objeto del intento o conspiración.

- *18 U.S.C. Sección 1028A- Robo de identidad agravado*

  (a) Ofensas- (1) En general- Quienquiera, durante y en relación con cualquier infracción grave enumerada en el inciso (c), transfiere, posee o utiliza a sabiendas, sin autoridad legal, un medio de identificación de otra persona, además del castigo. dispuesto para tal delito, ser condenado a una pena de prisión de 2 años.

- *18 U.S.C. Sección 2264- Restitución*

  (a) En general- No obstante, la sección 3663 o 3663A, y además de cualquier otra sanción civil o penal autorizada por la ley, el tribunal ordenará la restitución de cualquier delito en virtud de este capítulo.

  La orden de restitución conforme a esta sección ordenará al demandado que pague a la víctima (a través del mecanismo judicial apropiado) el monto total de las pérdidas de la víctima según lo determine el tribunal conforme a:

  (A) servicios médicos relacionados con la atención física, psiquiátrica o psicológica;

  (B) terapia física y ocupacional o rehabilitación;

  (C) transporte necesario, alojamiento temporal y gastos de cuidado infantil;

  (D) pérdida de ingresos;

  (E) honorarios de abogados, más los costos incurridos para obtener una orden de

protección civil; y

(F) cualquier otra pérdida sufrida por la víctima como resultado próximo de la ofensa.

Casos Relacionados

Caso 1

Evaldas Rimasauskas (United States Department of Justice, 2017) llevó a cabo un esquema de compromiso de correo electrónico comercial que se dirigía de manera creativa a dos compañías víctimas muy específicas. Inicialmente tuvo éxito, adquiriendo más de $100 millones en ganancias que conectó a varias cuentas bancarias en todo el mundo. Desde el año 2013 hasta aproximadamente el año 2015, Rimasauskas organizó un esquema fraudulento diseñado para engañar a las Compañías Víctimas, incluida una empresa multinacional de tecnología y una empresa multinacional de medios sociales en línea, para transferir fondos a cuentas bancarias controladas por Rimasauskas. Específicamente, Rimasauskas registró e incorporó una compañía en Letonia ("Compañía 2") que tenía el mismo nombre que un fabricante de hardware informático con sede en Asia ("Compañía 1"), y abrió, mantuvo y controló varias cuentas en bancos ubicados en Letonia y Chipre en nombre de la Compañía 2.

Posteriormente, se enviaron correos electrónicos fraudulentos de suplantación de identidad a empleados y agentes de *Victim Companies*, que regularmente realizaban transacciones multimillonarias con la Compañía 1, y ordenaban que el dinero que las Compañías Víctimas le debían a la Compañía 1 por bienes y servicios legítimos fuera enviado al banco de la Compañía 2 cuentas en Letonia y Chipre, controladas por Rimasauskas. Estos correos electrónicos pretendían ser de empleados y agentes de la Compañía 1 los cuales fueron enviados de cuentas diseñadas para cometer este fraude. Este esquema logró engañar a las Compañías

Víctimas para que efectuaran transferencias de dinero a distintas cuentas de banco. Después de que las Compañías Víctimas transfirieron fondos destinados a la Compañía 1 a las cuentas bancarias de la Compañía 2 en Letonia y Chipre, Rimasauskas causó que los fondos robados se transfirieran rápidamente a distintas cuentas bancarias en diferentes lugares del mundo, incluyendo Letonia, Chipre, Eslovaquia, Lituania, Hungría y Hong Kong. Rimasauskas también generó facturas falsificadas, contratos y cartas que aparentemente fueron ejecutadas y firmadas por ejecutivos y agentes de las Compañías de Víctimas, y que llevaban sellos corporativos falsos grabados con el nombre de las Compañías de Víctimas, que se presentaban a los bancos en apoyo del gran volumen de fondos que se transmitieron de manera fraudulenta mediante transferencia bancaria. Está acusado de un cargo de fraude electrónico y tres cargos de lavado de dinero, cada uno de los cuales conlleva una pena máxima de 20 años de prisión y un cargo de robo de identidad con agravantes, que conlleva un mínimo obligatorio de dos años de prisión.

Caso 2

Onyekachi Emmanuel Opara (United States Department of Justice, 2018e) fue sentenciado en la corte federal de Manhattan a 60 meses de prisión, dos años de libertad supervisada y $ 2.5 millones en restitución. Los cargos que se le dieron fueron por fraude electrónico. Opara y sus conspiradores intentaron estafar a las víctimas por más de $25 millones. Entre 2014 y 2016, Opara y su conspirador, David Chukwuneke Adindu, participaron en estafas de transacciones comerciales por correo electrónico (BEC) que se dirigieron a miles de víctimas en todo el mundo tales como: Estados Unidos, Reino Unido, Australia, Suiza, Suecia, Nueva Zelanda y Singapur.

Opara envió correos electrónicos falsos a empleados de las compañías víctimas que ordenaban que los fondos se transfirieran a cuentas bancarias específicas. Los correos electrónicos supuestamente pertenecían a supervisores de esas compañías o de proveedores externos con los que las compañías hacían negocios. En realidad, los correos electrónicos se enviaron desde cuentas de correo electrónico con nombres de dominio muy similares a los de las empresas y proveedores, o se modificaron los metadatos de los correos electrónicos para que parecieran que los correos electrónicos habían sido enviados desde direcciones de correo electrónico legítimas. Después de que las víctimas transfirieron los fondos como se indica en los correos electrónicos falsos, los fondos se retiraron rápidamente o se transfirieron a otras cuentas bancarias controladas por los participantes del esquema. En total, los participantes de la estafa de BEC intentaron robar más de $ 25 millones a víctimas de todo el mundo.

Para promover las estafas de BEC, Opara creó cuentas en sitios web de citas y entabló relaciones románticas en línea con personas en los Estados Unidos al presentarse como una joven atractiva llamada "Barbara". Barbara instruiría a estas personas en los Estados Unidos para enviar su dinero al extranjero y / o para recibir dinero de las estafas de BEC y reenviar los ingresos a otros participantes del esquema ubicados en el extranjero. Por ejemplo, una víctima con quien Opara inició una relación romántica envió más de $ 600,000 del dinero propio de la víctima a cuentas bancarias controladas por los participantes del esquema bajo la dirección de Opara.

Caso 3

Joshua Philips (United States Department of Justice, 2018d), fue arrestado el 7 de marzo de 2018 en el Distrito Norte de Georgia y fue procesado por los cargos de fraude bancario,

lavado de dinero y fraude de compromiso electrónico empresarial (BEC). Alrededor de julio de 2017 y agosto de 2017, el acusado y otros atacaron a una persona en Long Island (John Doe 1) que estaba involucrado en una transacción de bienes raíces relacionada con la compra de una propiedad en Massapequa, Nueva York, y su Abogado de bienes raíces (John Doe 2), quien facilitó la compra.

El 23 de agosto de 2017, o alrededor de esa fecha, John Doe 1 recibió un correo electrónico de la cuenta de correo electrónico de John Doe 2 en el que se le preguntaba: ¿Con respecto a los fondos de cierre, está disponible actualmente? Después de responder que los fondos estaban disponibles, John Doe 1 recibió un correo electrónico el 24 de agosto de 2017, desde la cuenta de correo electrónico de John Doe 2, se le indicó que "vaya a su sucursal local dentro del día e inicie una transferencia bancaria de los fondos a mi cuenta de depósito en garantía del abogado". El correo electrónico proporcionó información para una cuenta bancaria que era, de hecho, en el control de uno de los conspiradores del acusado.

El 28 de agosto de 2017, John Doe 1 envió una transferencia bancaria por un monto de $84,000 a la cuenta bancaria. El conspirador recibió el dinero y transfirió una parte de este a Philips, quien luego envió una parte de este al extranjero. John Doe 2 ha informado a los agentes de la ley que no envió el correo electrónico del 24 de agosto y que los detalles de la cuenta bancaria no pertenecen a ninguna cuenta que esté bajo su control. Como parte de los esquemas más amplios habilitados por el sistema cibernético, Philips transfirió ilegalmente el dinero obtenido de manera fraudulenta en el extranjero, incluso a varias cuentas bancarias extranjeras y para comprar automóviles usados para una empresa de importación /exportación en Nigeria.

Herramienta de investigación

1. Forensic Tool Kit (FTK)

FTK está destinado a ser una solución forense informática completa. Proporciona a los investigadores una agregación de las herramientas forenses más comunes en un solo lugar. Ya sea que intente descifrar una contraseña, analizar correos electrónicos o buscar caracteres específicos en los archivos. FTK proporciona una interfaz intuitiva para el análisis de correo electrónico para profesionales forenses. Esto incluye tener la capacidad de analizar correos electrónicos para ciertas palabras, análisis de encabezado para la dirección IP de origen, etc. (Access Data, 2018)

SECCIÓN 3: SIMULACIÓN

La simulación de un delito es la reconstrucción de los hechos de forma que sea igual o parecido a como fue cometido. En muchas investigaciones se utiliza esta técnica para ir más allá del acto y observar de manera clara y precisa como ocurrieron los hechos. Es una técnica la cual se obtiene mucha información que no se aprecia a simple vista y que los investigadores la pueden utilizar para el manejo apropiado de la escena criminal.

En este caso se ha investigado un esquema de fraude de compromiso de correo electrónico empresarial (BEC, por sus siglas en inglés) en qué CEO, controladores y otros en las empresas de los Estados Unidos han sido identificados como víctimas. Los perpetradores de esta investigación fueron identificados por Stanley Hugochukwu Nwoke, Adeyemi Odufuye, Olumuyiwa Yahtrip Adejumo, entro otros conspiradores. Los mismos utilizaban técnicas cibernéticas sofisticadas para estafar a las empresas estadounidenses, incluidas las empresas en Connecticut. En un esquema de compromiso de correo electrónico empresarial, uno o más individuos se dirigen a una empresa o individuo específico haciéndose pasar por una entidad confiable en una comunicación electrónica para obtener información sensible, dinero o propiedad de la víctima.

Este fraude da comienzo cuando los perpetradores en la primera fase del delito realizaban una investigación extensa de la empresa victima que quería defraudar, la cual podía tomas meses o semanas (dependiendo el caso) en recopilar información de estas. Uno de los requisitos que consideraban para cometer este delito era encontrar compañías las cuales no tenían físicamente la oficina del CEO presente en la empresa, si no que la compañía estuviera en un país o estado

diferente a la oficina de este. Esto con el propósito que pudieran realizar la falsa representación con efectividad. Posteriormente del paso anterior, procedían al siguiente paso. En este paso como dato importante luego de estar al tanto que el CEO no está dentro de la empresa procedían a identificar al encargado en el área de finanzas.

Luego de tener la persona encargada del área donde se pretende realizar la comisión del delito, el perpetrador comienza a enviar correos electrónicos a esta persona. En estos correos electrónicos el mensaje que se enviaba decía que al supuesto CEO se le había presentado un asunto importante en el cual solicitaba que cierta cantidad monetaria se le transfiriera a una cuenta de banco, la cual enviaba en el mensaje junto con la información de esta. La persona victima al recibir el correo electrónico y ver que es enviado por el supuesto CEO de la empresa procedía a realizar la transferencia convirtiéndose en una víctima de este esquema de fraude.

Por otro lado, Odufuye, Adejumo y Nwoke mantenían comunicación vía correo electrónico y redes sociales para mantenerse al tanto de lo que estaba ocurriendo. Estos compartían los correos electrónicos para cometer este fraude. Todos realizaban el mismo proceso o rol para desarrollar el delito. (Véase figura 1)

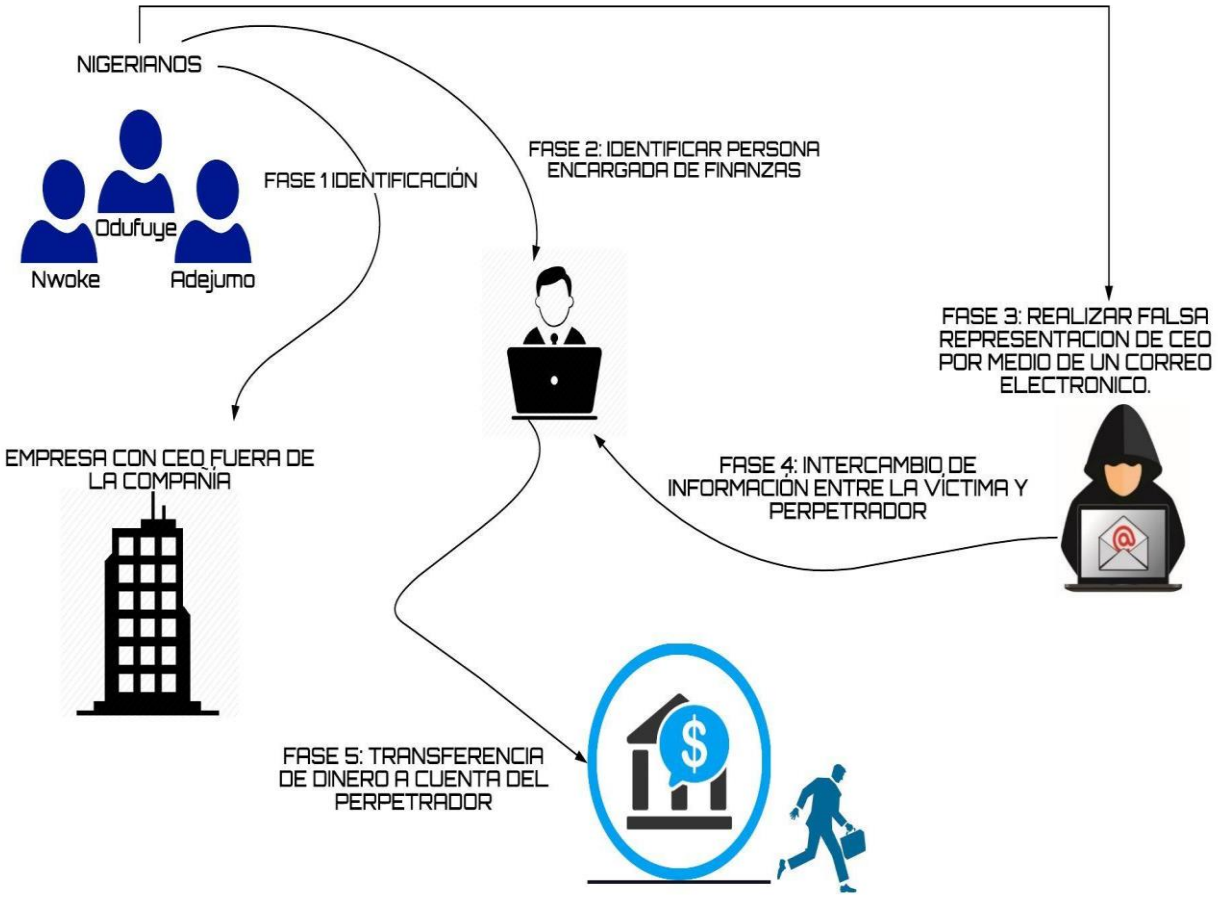

Figura 1: Diagrama del esquema BEC

SECCIÓN 4: INFORME DEL CASO

Resumen Ejecutivo

La fiscalía del estado de Connecticut está investigando el caso Estados Unidos v. Adejumo, Odufuye & Nwoke bajo un esquema de fraude por correo electrónico. David T. Huang es el fiscal asignado al caso, quien contactó la examinadora de fraude Dinoshka Valentín, del laboratorio forense DVF para que analizara la evidencia recolectada en la investigación. El fiscal del caso entregó un pendrive a la examinadora Valentín, el cual tenía almacenado una imagen del disco duro de una computadora que utilizaban los perpetradores.

Objetivo

La examinación forense digital tiene como objetivo analizar, recopilar y preservar la evidencia encontrada en la imagen del disco duro para fines investigativos. En el análisis se utilizarán técnicas forenses las cuales nos ayudaran a descifrar el que, como, cuando, por qué y por quien fueron cometidos los hechos expuestos en la investigación.

Alcance

El fiscal David T. Huang hace entrega de la evidencia a la examinadora el día 4 de diciembre de 2018. La evidencia recolecta será sometida bajo el análisis forense con el propósito de detallar lo ocurrido. En el caso se estará analizando una imagen del disco duro para examinar posibles correos electrónicos enviados o alguna otra evidencia que conecte a los perpetradores con los hechos ocurridos. Para esta examinación se utilizará la herramienta *FTK Imager* para el análisis forense de la evidencia. Esta aplicación es utilizada en investigaciones para analizar, reconstruir y recuperar las evidencias digitalmente. La herramienta FTK Imager es una

plataforma de investigaciones digitales aprobada por tribunales, que está diseñada para ser veloz, analítica y contar con escalabilidad de clase empresarial (Access Data, 2018).

Datos del caso

1. Número de caso: 16-cr-00232 / 3:18-cr-00082
2. Examinador Forense: Dinoshka Valentin
3. Cliente: Tribunal de los Estados Unidos, Distrito Sur de Connecticut
4. Representante del cliente: Fiscal David T. Huang

Descripción de los dispositivos utilizados

En esta examinación forense para el caso United States v. Adejumo, Odufuye & Nwoke se analizó la evidencia obtenida por los agentes del FBI incautada al momento de la investigación. Los dispositivos utilizados fueron los siguientes:

1. Computadora portátil (Laptop) marca Acer modelo Aspire ES 15. Consta del Sistema operativo Windows 8. Tiene un procesador Intel Core i3 de 2.3 GHz con 4GB DDR3L y 1T HDD. La misma consta con los programas y herramientas utilizados.
2. USB Drive, marca Verbatim con capacidad de almacenaje de 32 GB.

Resumen de Hallazgos

Dentro de esta sección se presentan los hallazgos que se localizaron mediante el análisis forense del Pendrive Verbatim, en el cual se encuentra almacenada una imagen del disco duro de la computadora de los perpetradores entregada por el Fiscal del Tribunal de Circuito de Connecticut a la examinadora de fraude. Utilizando la herramienta FTK Imager se encontró lo siguiente:

1. Capturas de correos electrónicos que los perpetradores enviaban con un correo falso haciéndose pasar por el CEO de la compañía víctima. Dentro de estos correos se ve el mensaje como es contestado por el empleado de la compañía víctima. (Ver figuras 2 a la 5)

2. De igual modo, se observa documentos PDF revelando información acerca de transferencias de dinero a bancos fuera del país y formularios que el victimario les enviaba a sus víctimas. (Ver figuras 6 y 7)

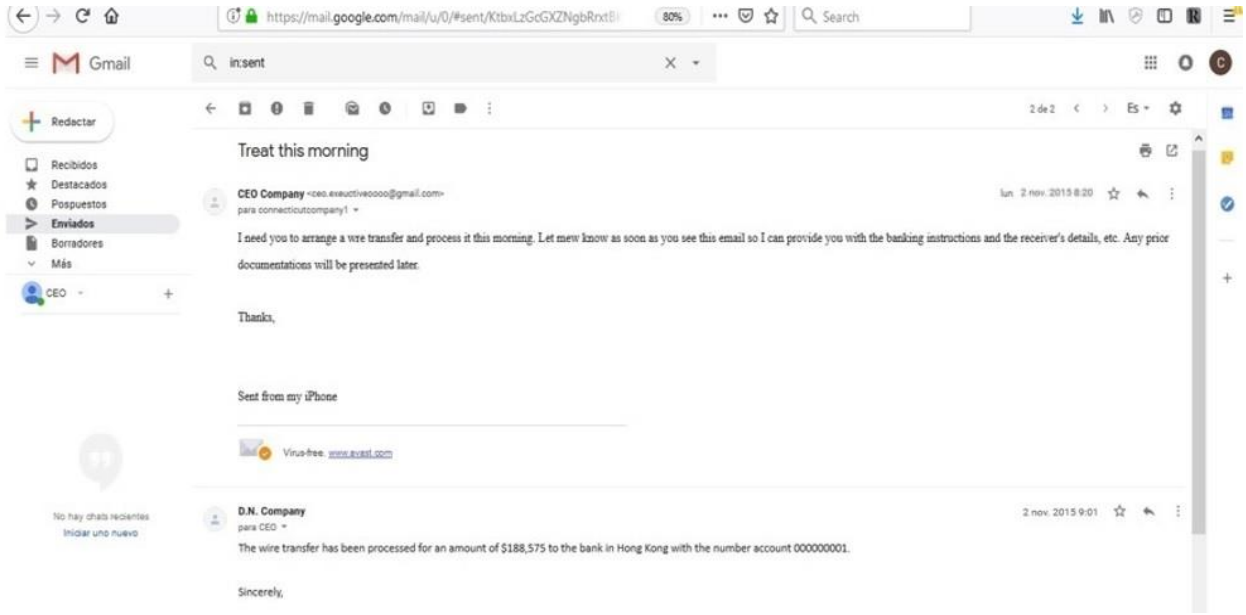

Figura 2: Primer correo electrónico enviado a Compañía Víctima 1.

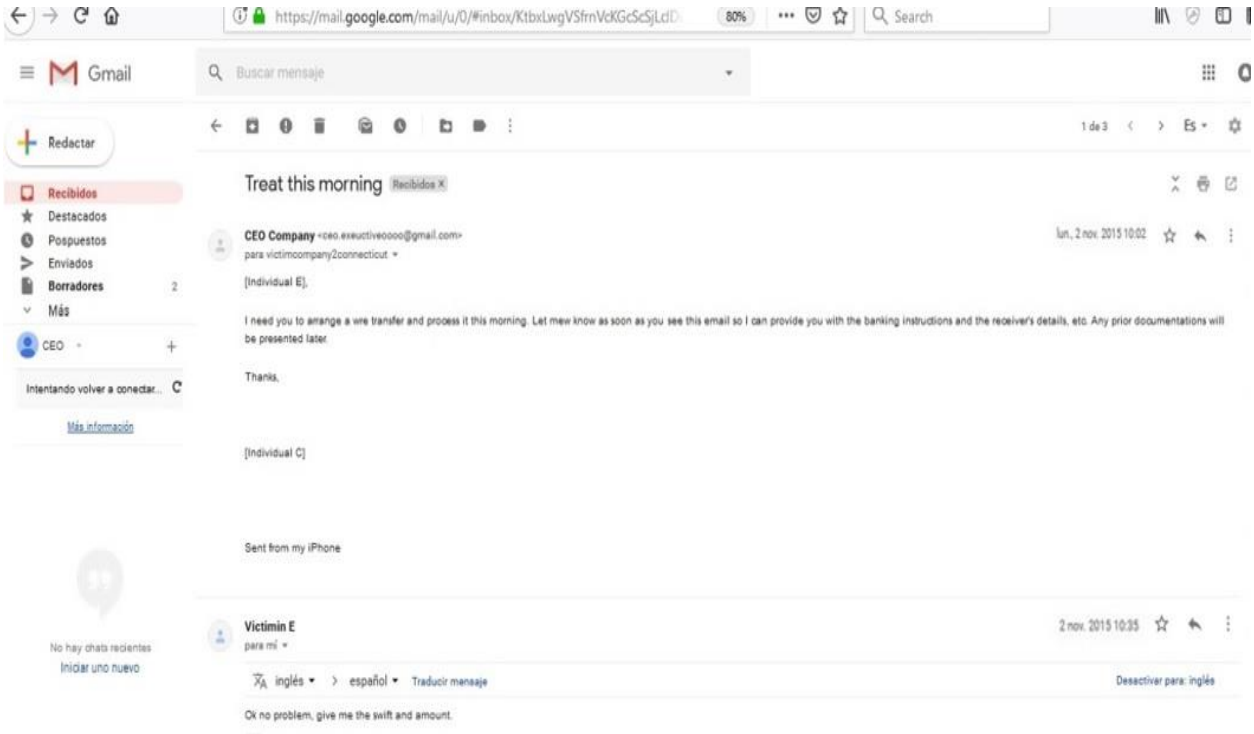

Figura 3: Email enviado a Compañía Víctima 1 solicitando una transferencia de dinero.

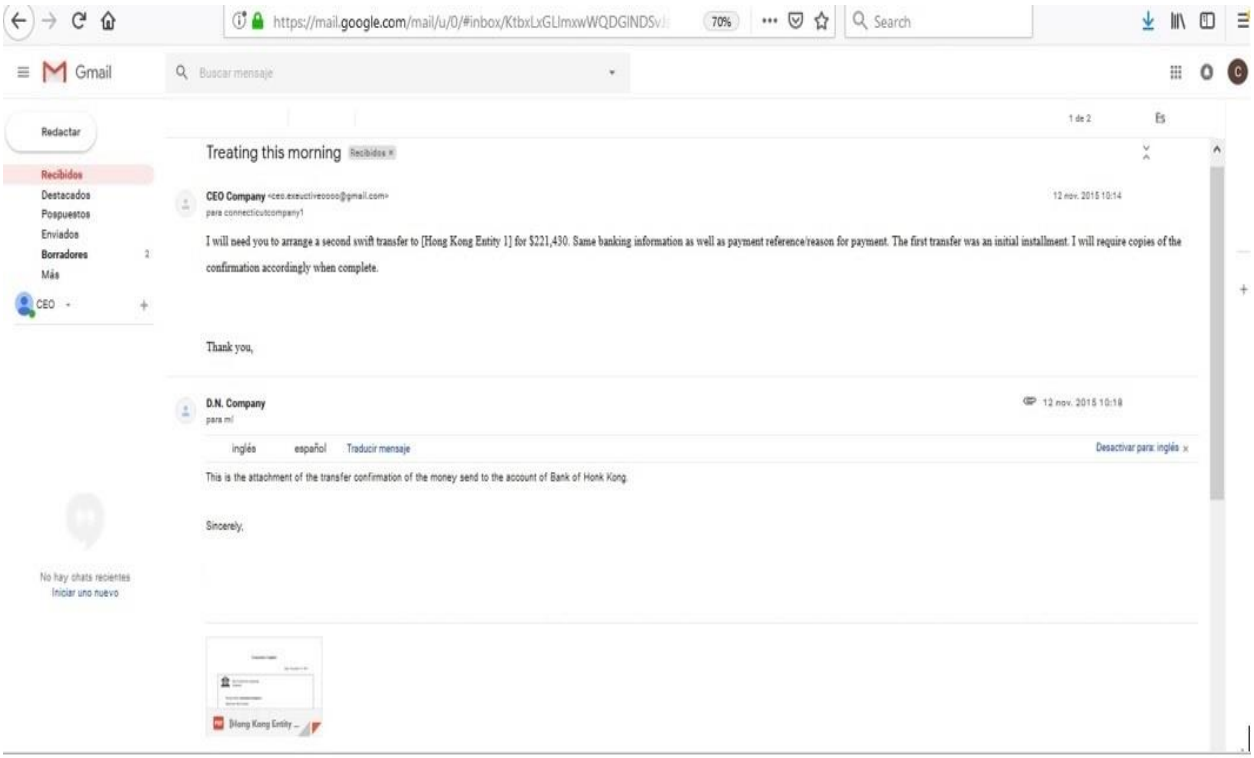

Figura 4: Correo electrónico enviado a Compañía Víctima 1, junto con instrucciones de cuenta de banco extranjera.

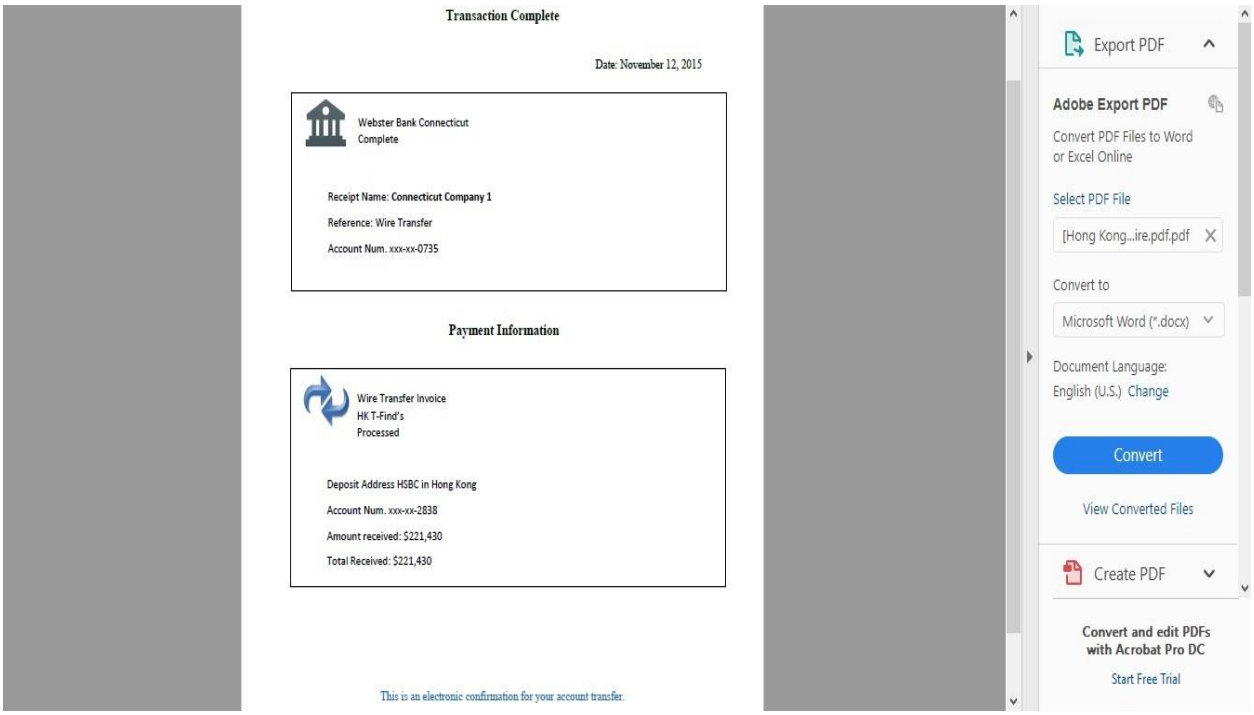

Figura 5: Documento PDF enviado en el correo electrónico de aprobación de transferencia bancaria.

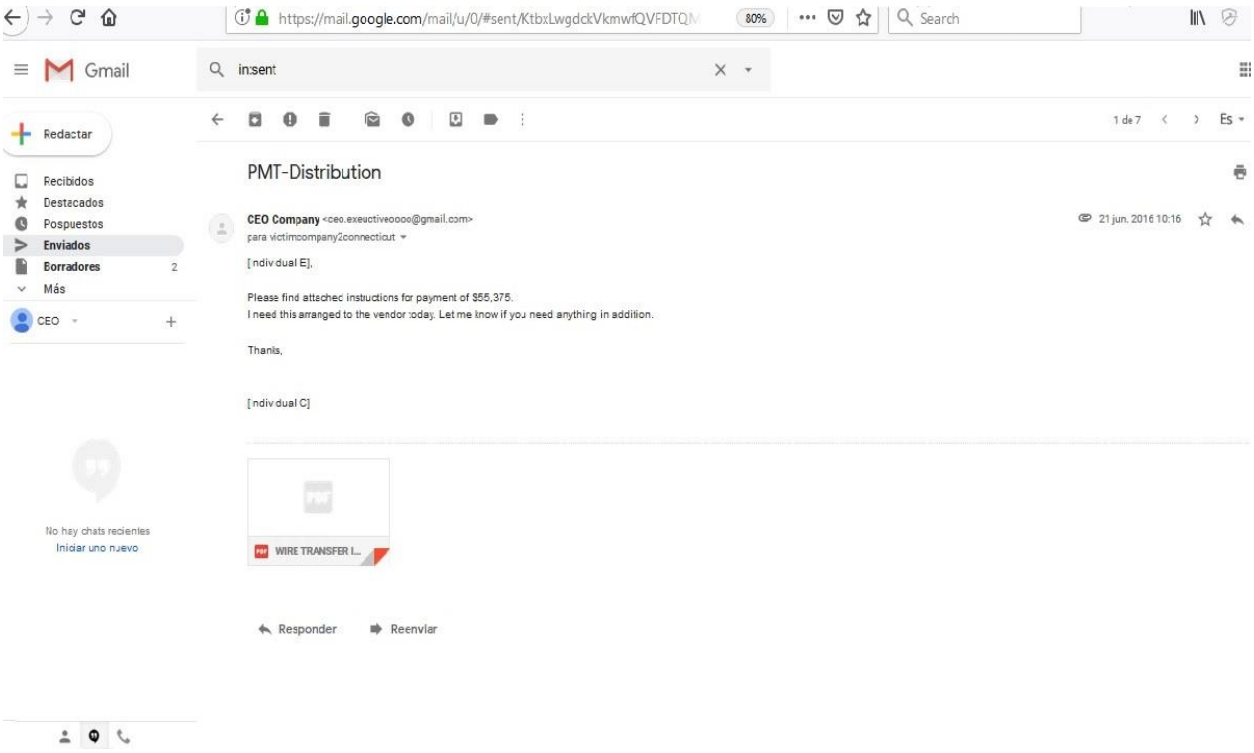

Figura 6: Correo electrónico enviado a Compañía Víctima 2.

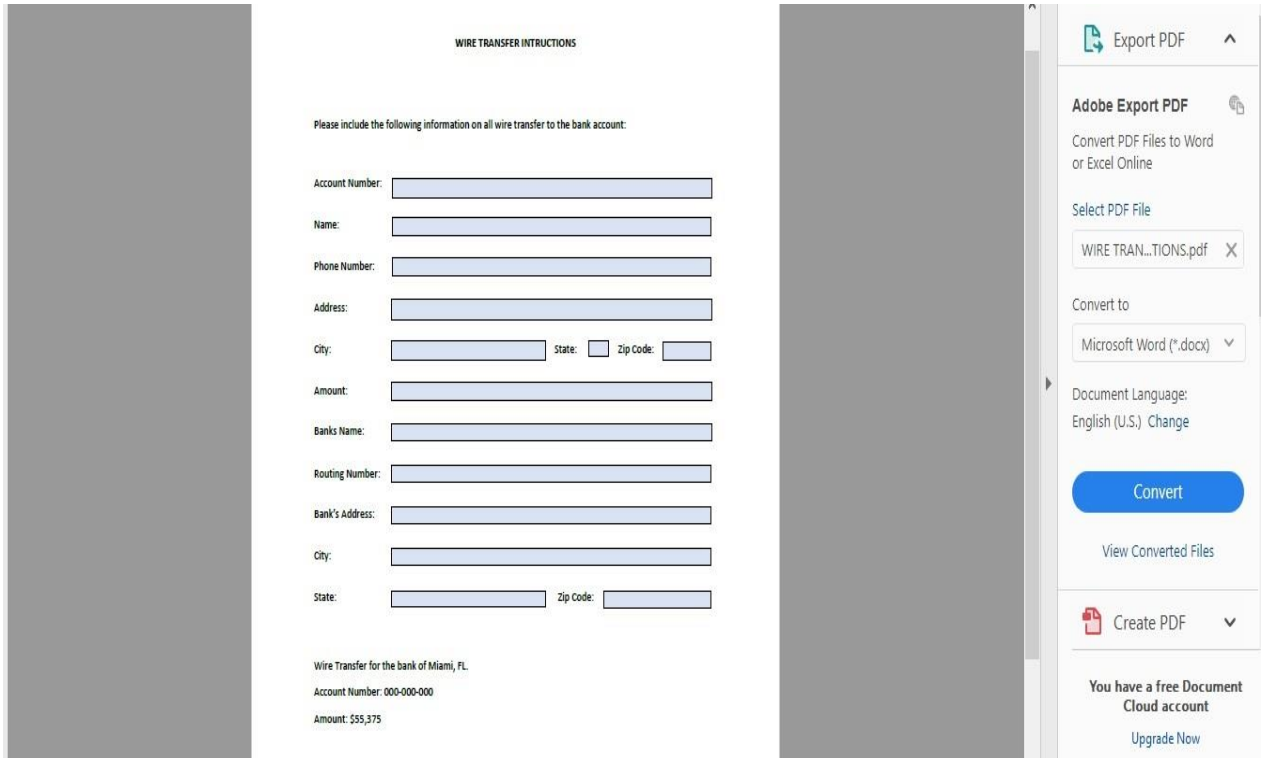

Figura 7: Formulario PDF con instrucciones para realizar una transferencia de dinero a banco extranjero.

Cadena de Custodia

El laboratorio forense DVF está a cargo de cumplir con los protocolos necesarios para analizar, preservar y custodiar la evidencia. La cadena de custodia tiene como propósito proteger los archivos recopilados en la investigación para que no sufran alguna contaminación, daños, alteraciones o destrucciones y los mismos sean procesados de forma satisfactoria ante un tribunal o algún dictamen pericial.

Primer Evento

1. Descripción del evento: Evidencia entregada por el Fiscal David T. Huang al Laboratorio Forense DVF, para ser analizado por la examinadora Dinoshka Valentin. La evidencia se encuentra en un USB Drive.
2. Evento verificado por: examinadora digital Dinoshka Valentin y Fiscal del Distrito de Connecticut David T. Huang.
3. Fecha de comienzo: 6 de diciembre 2018 4:50 p.m.
4. Fecha de terminación: 6 de diciembre de 2018 4:56 p.m.
5. Lugar de origen: Tribunal de Circuito de Connecticut.
6. Destino: Laboratorio Forense DVF.

Segundo Evento

1. Descripción del evento: Creación de número de caso y asignación de evidencia.
2. Evento verificado por: Dinoshka Valentín
3. Asignar número al caso: 2016-232
4. Fecha de comienzo: 6 de diciembre 2018 5:00 p.m.
5. Fecha de terminación: 6 de diciembre de 2018 5:05 p.m.
6. Lugar de origen: Laboratorio Forense DVF.
7. Destino: Laboratorio Forense DVF.

Tercer Evento

1. Descripción del evento: Proceso de análisis de evidencia
2. Evento verificado por: Dinoshka Valentín
3. Asignar número al caso: 2016-232

4. Fecha de comienzo: 6 de diciembre 2018 5:19 p.m.
5. Fecha de terminación: 6 de diciembre de 2018 5:32 p.m.
6. Lugar de origen: Laboratorio Forense DVF.
7. Destino: Laboratorio Forense DVF.

Cuarto Evento

1. Descripción del evento: Devolución de la pieza USB Drive analizada. Entrega realizada por la examinadora forense Dinoshka Valentin y recibida por el Fiscal David T. Huang
2. Evento verificado por: Fiscal David T. Huang
3. Número de caso asignado: 2016-232
4. Fecha de comienzo: 7 de diciembre 2018 1:00 p.m.
5. Fecha de terminación: 7 de diciembre de 2018 1:40 p.m.
6. Lugar de origen: Laboratorio Forense DVF.
7. Destino: Tribunal de Circuito de Connecticut.

Procedimiento

Para el análisis de la pieza investigada se utiliza la herramienta forense FTK Imager 3.1.x en la computadora virtual Windows XP. El primer procedimiento realizado fue crear una copia de la evidencia obtenida en el USB Drive. Esta copia se crea para que la evidencia que se encuentra guardada dentro del mismo no sea alterada o dañada al momento de comenzar el análisis de investigación forense. La imagen que se crea será una exacta a la original suministrada en el pendrive. (Véase figuras 8 a la 11)

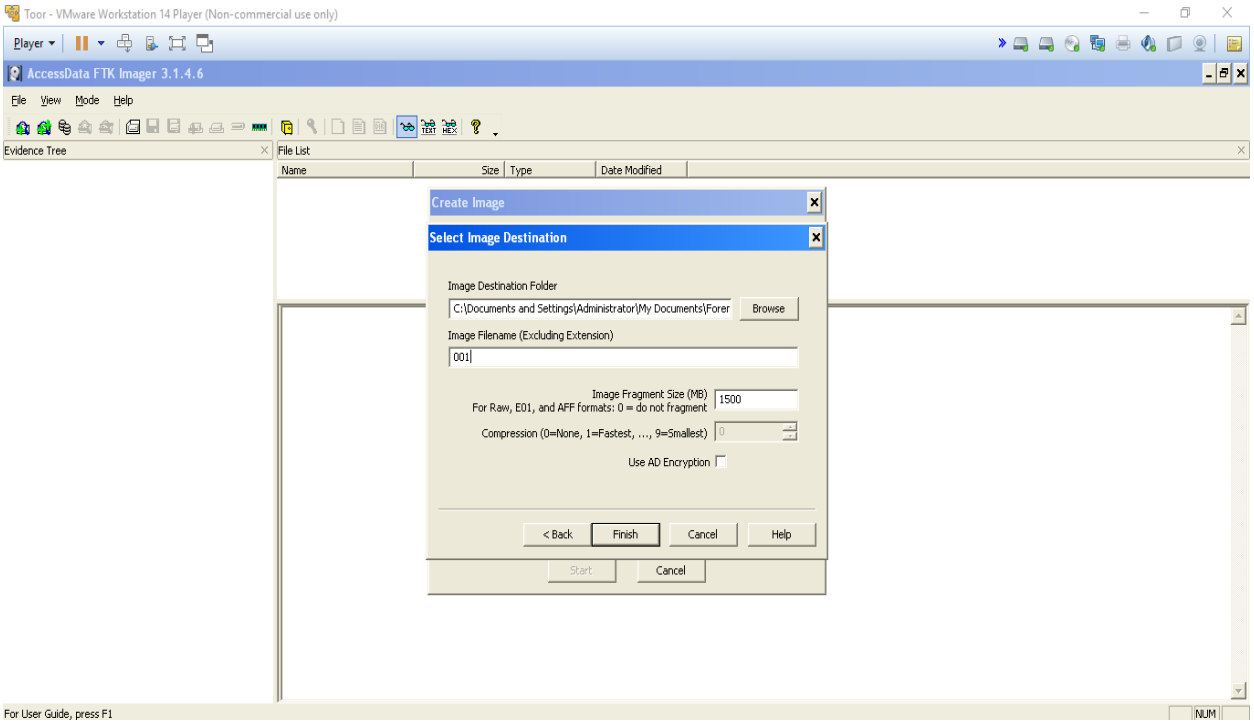

Figura 8: Creación de la imagen

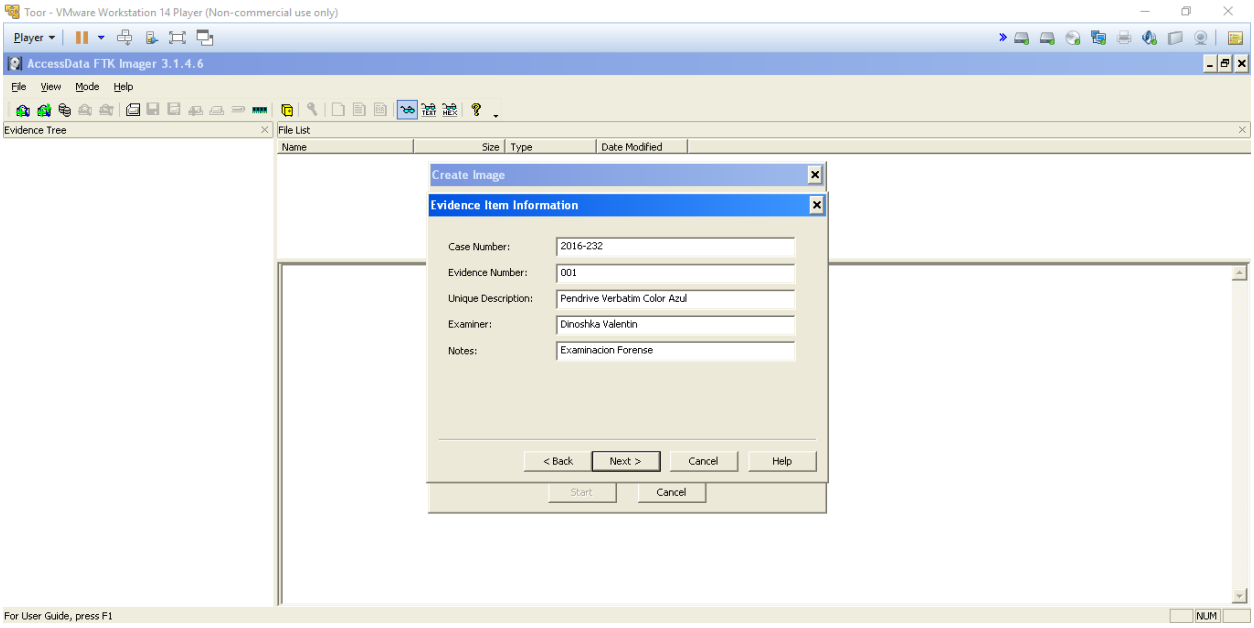

Figura 9: Creación de imagen, información de la evidencia.

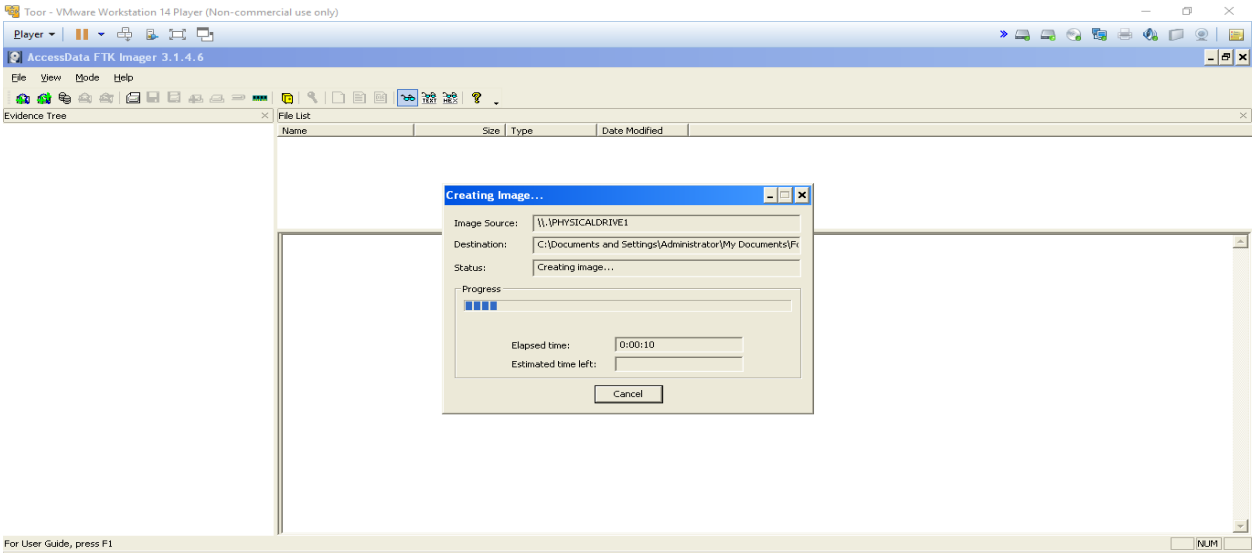

Figura 10: Creación de la imagen

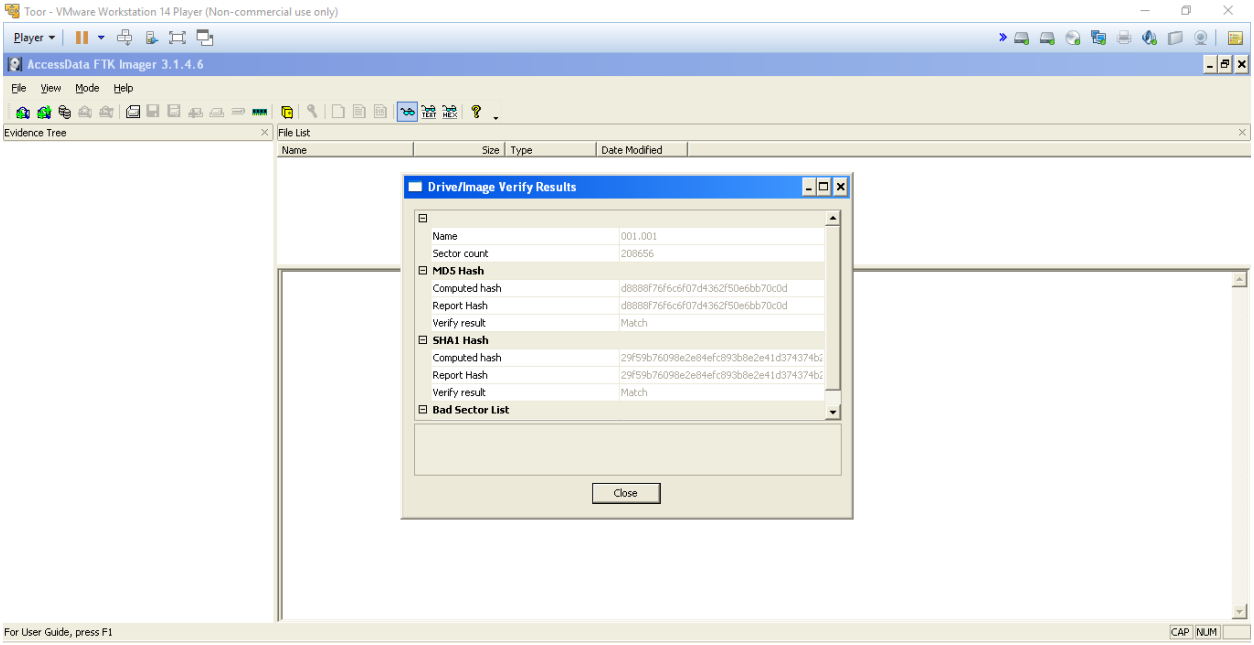

Figura 11: Resultados creación imagen.

Una vez creada la imagen se procede a analizar los archivos. Dentro de estas figuras analizadas se encuentran los correos electrónicos que los perpetradores les enviaron a las empresas víctimas realizando el esquema de fraude BEC. En estos correos electrónicos el victimario le pide a la empresa víctima que realice transferencias bancarias por ciertas cantidades

de dinero a cuentas de banco fuera de la compañía. En algunos casos se observa cuando la víctima responde los correos y les realizan las transferencias a estas cuentas. (Véase figuras de la 12 a la 15)

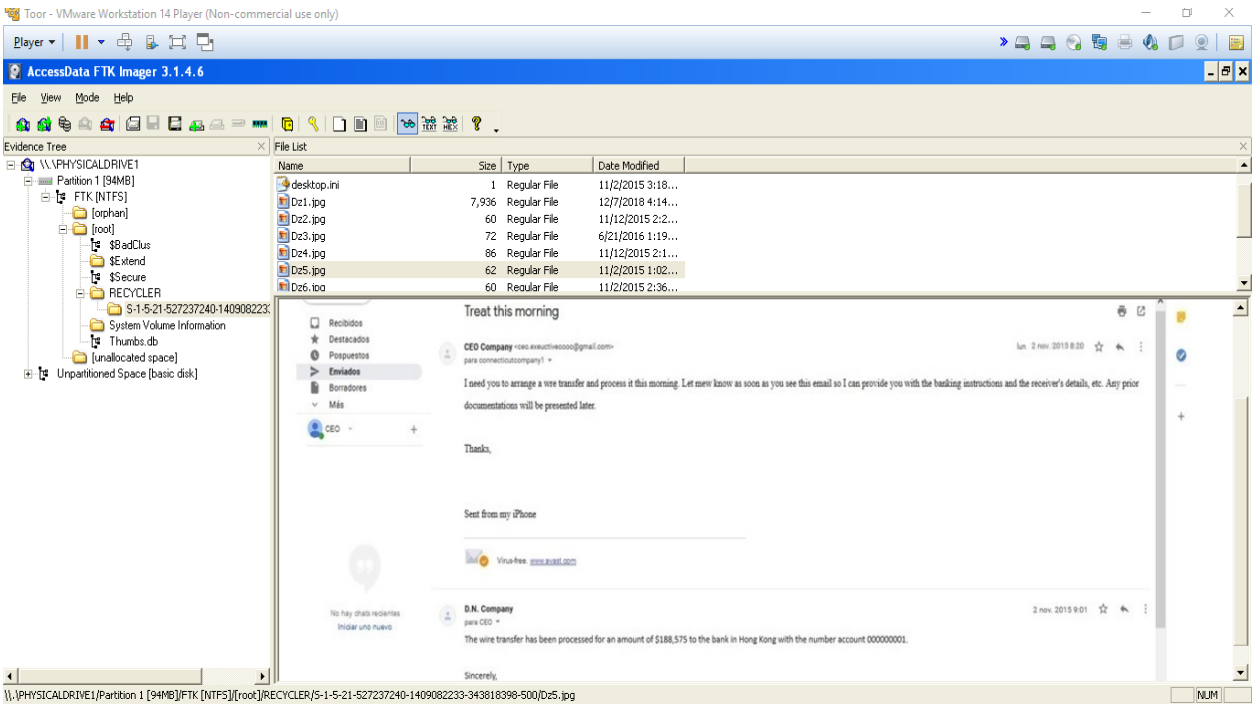

Figura 12: Análisis evidencia. Correos electrónicos enviado Compañía Víctima 1.

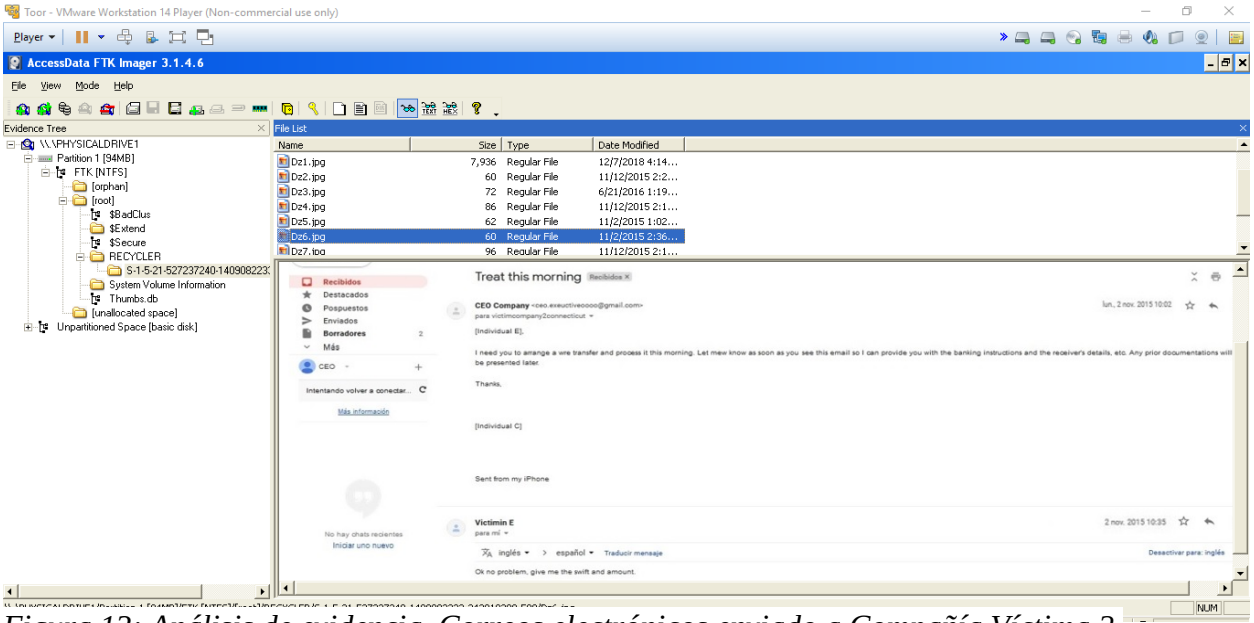

Figura 13: Análisis de evidencia. Correos electrónicos enviado a Compañía Víctima 2.

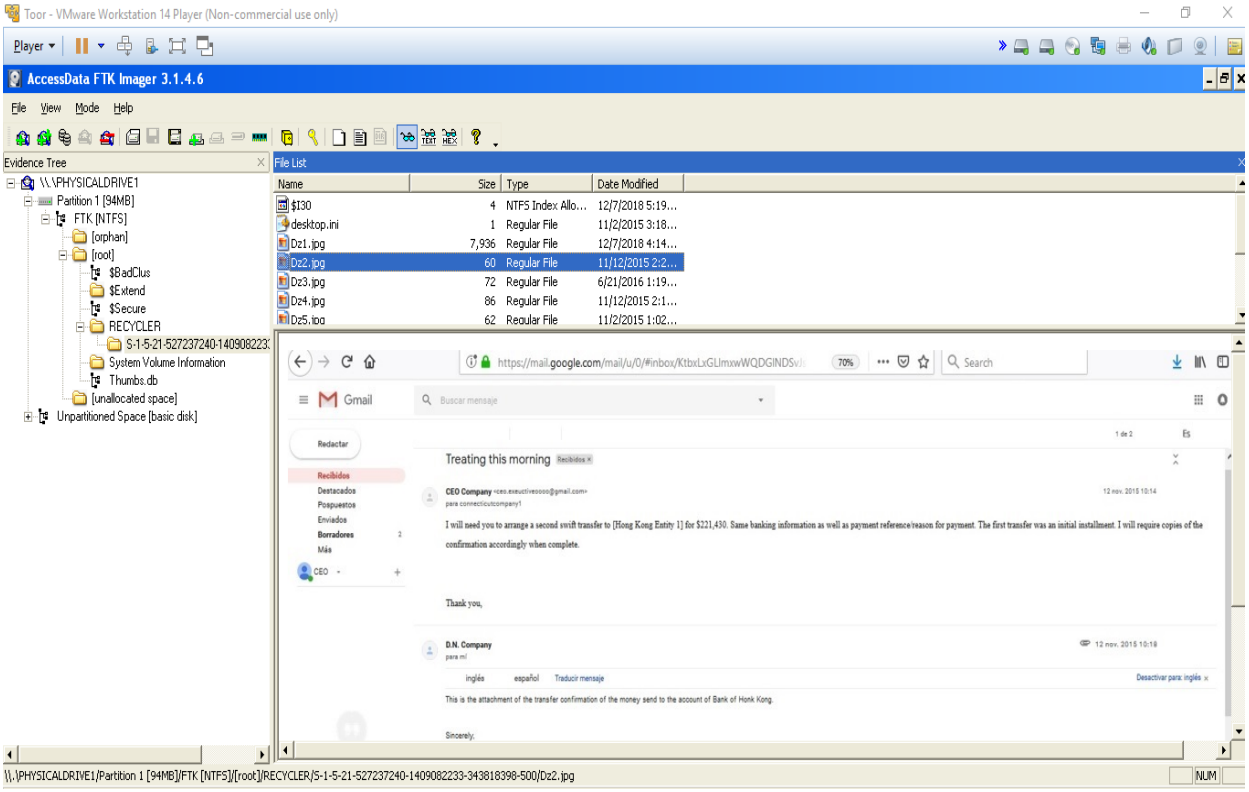

Figura 14: Correo electrónico enviado el día 12 de noviembre de 2015.

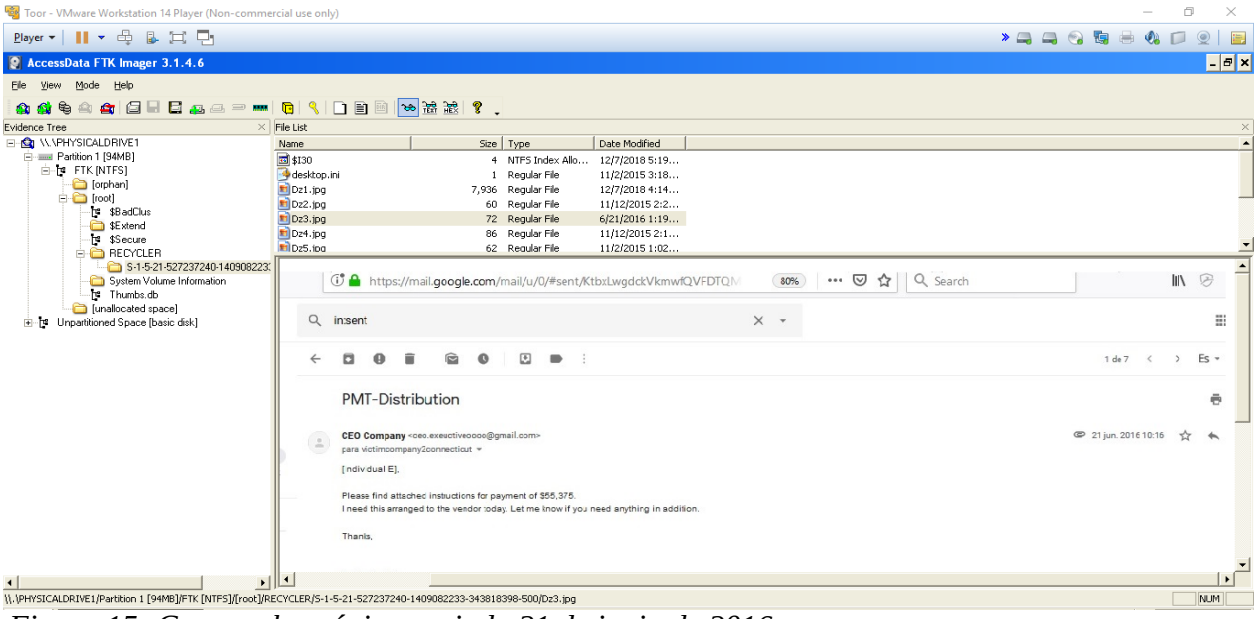

Figura 15: Correo electrónico enviado 21 de junio de 2016.

En este documento (véase figura 16) se encuentra una transacción que proceso la compañía victima 1 a Odufuye y Nwoke a una cuenta bancaria en Hong Kong. Este archivo fue adjunto en una conversación vía correo electrónico por estos y la compañía víctima

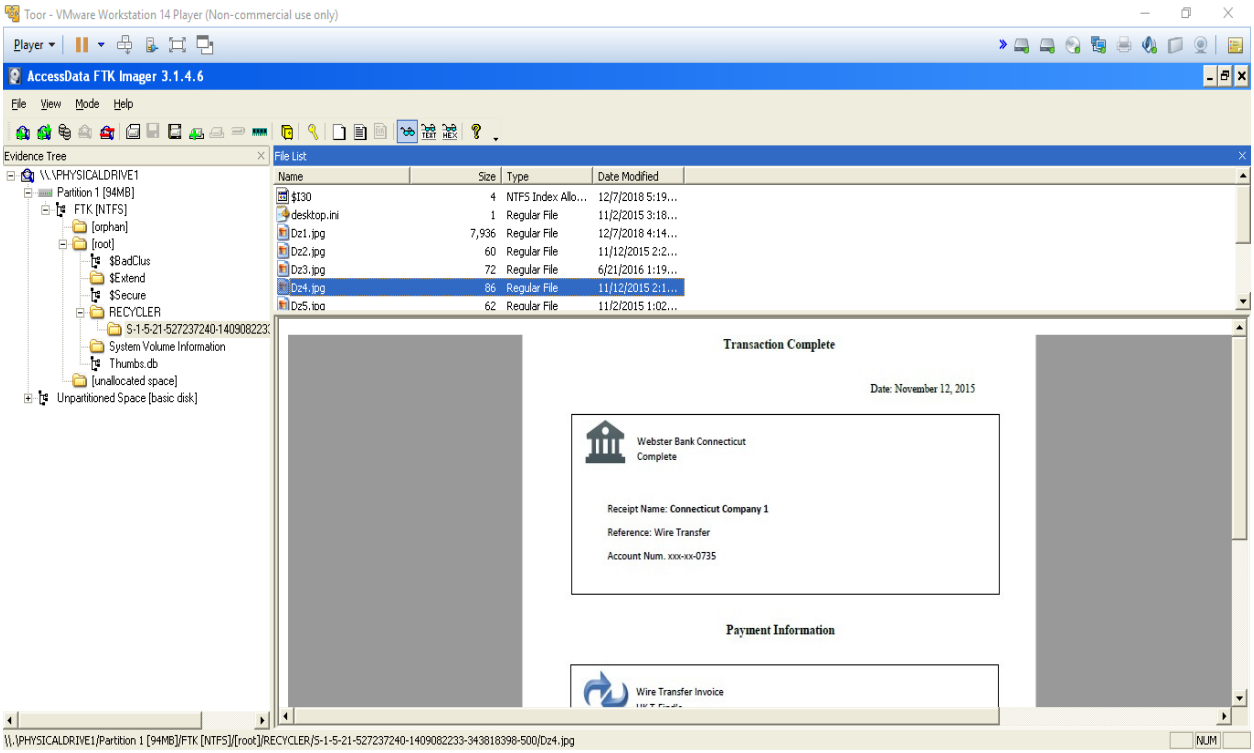

Figura 16: Archivo PDF de transacción procesada a un banco en Hong Kong.

En la figura 17 se muestra la evidencia capturada de un documento/formulario con instrucciones para realizar una transferencia bancaria electrónica. Este documento fue adjunto a un correo electrónico que se envió. (Véase figura 17)

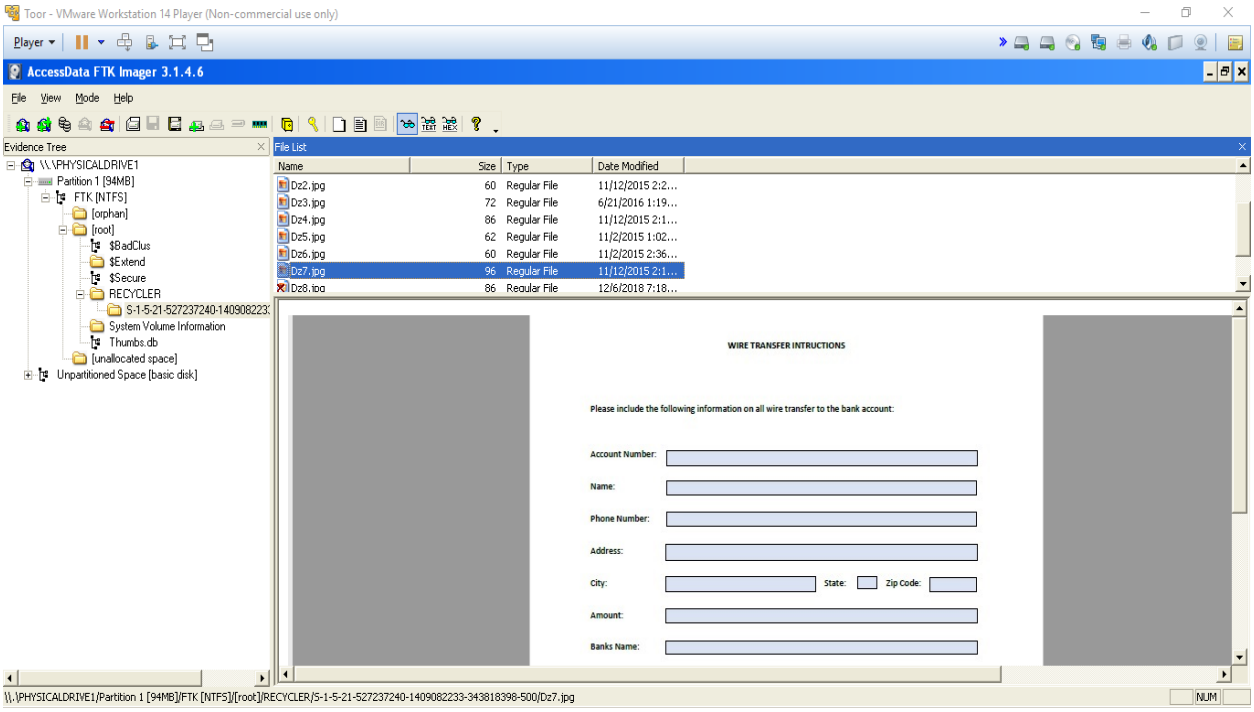

Figura 17: Documento en PDF de instrucciones para realizar una transferencia electrónica.

Luego de observar esta evidencia se exporta como se ve a continuación. (Véase figura 18 a la 22)

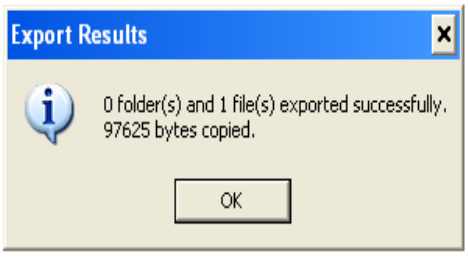

Figura 18: Exportación exitosa de la evidencia

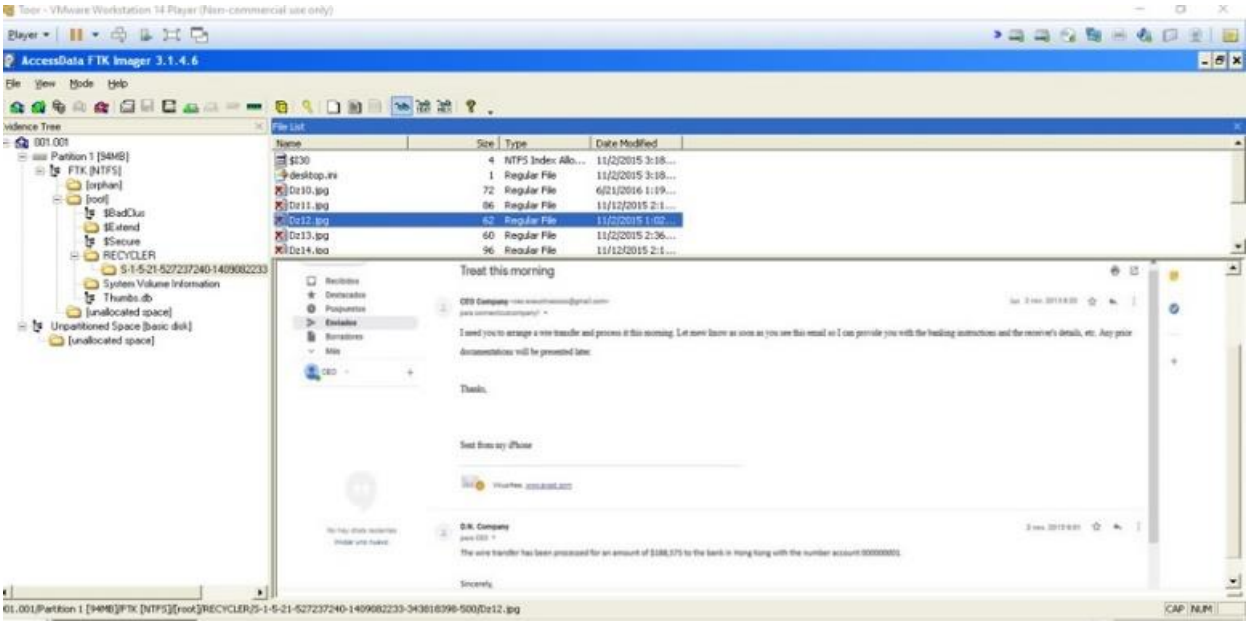

Figura 19: Evidencia exportada

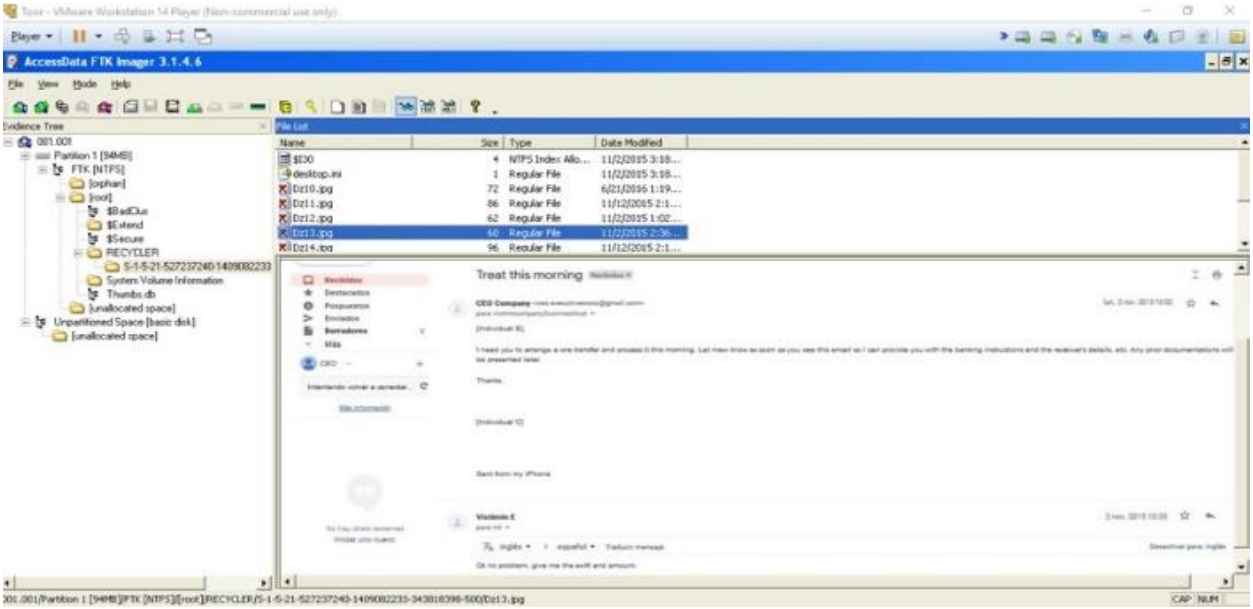

Figura 20: Evidencia Exportada

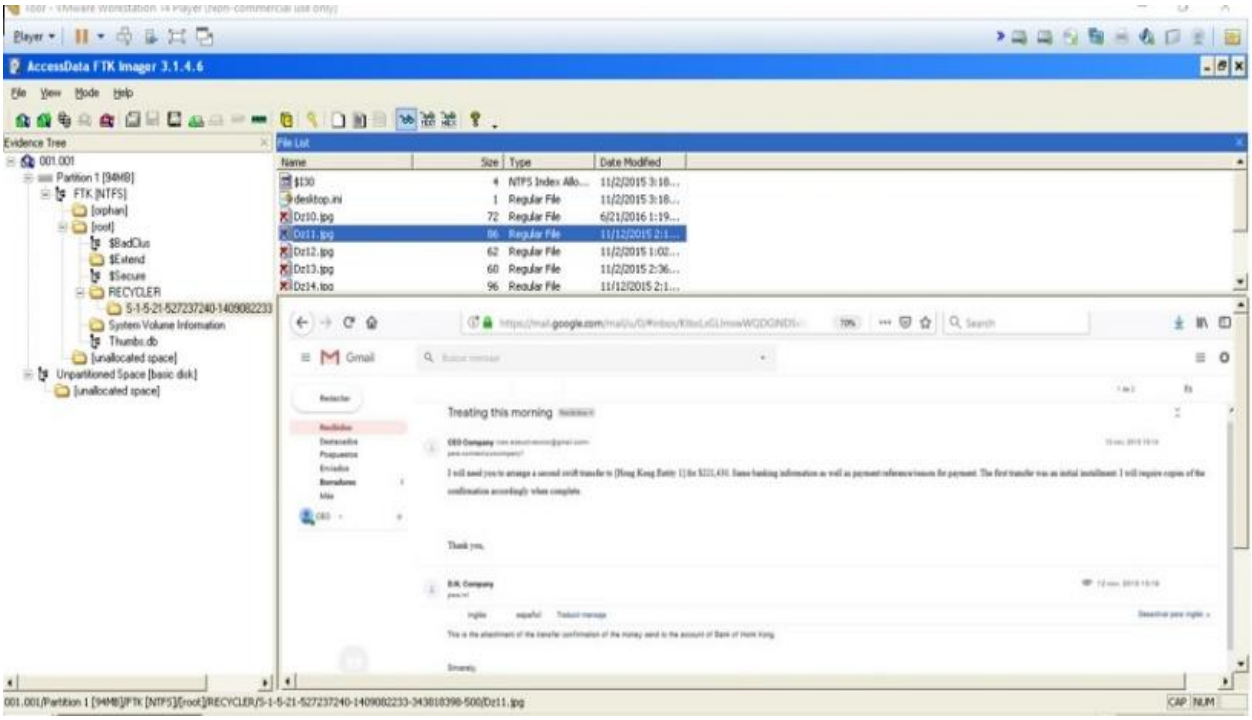

Figura 21: Evidencia Exportada

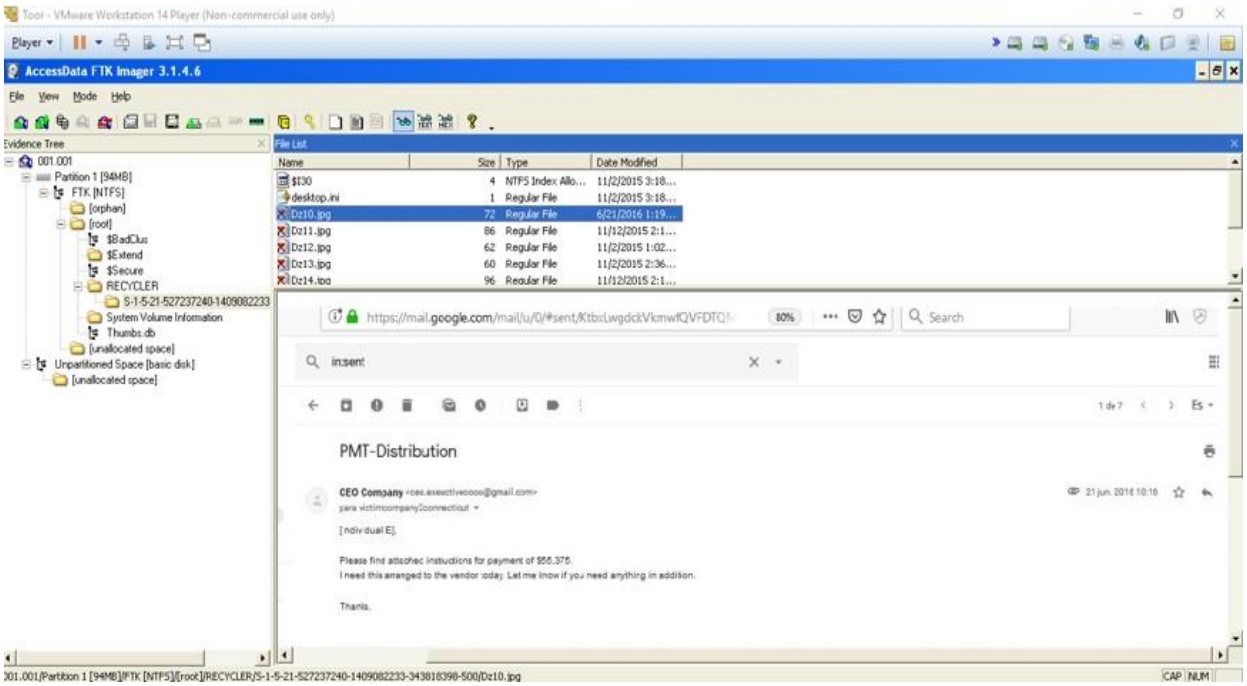

Figura 22: Evidencia Exportada

Conclusión

Después de analizar la imagen del disco duro almacenado en el USB Drive entregado por el Fiscal David T. Huang, se entiende que los acusados Odufuye, Adejumo y Nwoke enviaron diversos correos electrónicos a compañías ejecutivas haciéndose pasar por el CEO de la empresa, con el propósito que las compañías les enviaran transferencias monetarias a cuentas bancarias bajo el nombre de los perpetradores. Con los datos recopilados se pretendía verificar más allá de duda razonable que estos acusados conspiraron para cometer este esquema de fraude. Con esta examinación digital realizada se relaciona a los acusados con el esquema de fraude empresarial por medio de correo electrónico investigado. Este análisis debe ser corroborado por el tribunal para que se añada junto a las otras evidencias que se consideran pertinentes a la investigación en general.

SECCIÓN 5: DISCUSIÓN DEL CASO

Como mencioné anteriormente este caso trata acerca de un esquema de fraude por medio de correos electrónicos. Dentro de nuestra sociedad hoy día la tecnología ha evolucionado a través de los años, creando nuevos cambios y abriendo paso para que el fraude electrónico se desarrolle con gran auge. En los tiempos pasados la tecnología no era tan accesible a las personas, con estas evoluciones ya todos tenemos artefactos electrónicos por el cual nos podemos comunicar ya sea por llamadas, textos, redes sociales o correos electrónicos. Este esquema de "Business Email Compromise" se ha convertido en una modalidad durante los últimos años. El mismo se basa en que el perpetrador se hace pasar por un alto ejecutivo de la empresa y envía correos electrónicos a la supuesta compañía donde es jefe para que los mismos realicen una transferencia bancaria al número de cuenta que este les brindaba. Lo más sorprendente de estos casos es que la víctima no percibe la dirección del dominio la cual recibió el correo electrónico pensando que es un mensaje confiable y procede a realizar la transferencia.

Entre los acusados del caso se encontraba Odufuye quien había realizado su Maestría en Sistemas de Información en Seguridad. Observando este detalle del trasfondo del perpetrador podemos destacar que tiene un amplio conocimiento sobre el acto delictivo en el cual estaba incurriendo. Con este análisis se fundamenta como el fraude adquiere mayor acción en este esquema debido a la educación que presenta el perpetrador relacionada al tema estudiado. Para realizar este tipo de delito debe haber ciertos conocimientos los cuales Odufuye los poseía por medio de su educación en el área de tecnología. Por tal razón este esquema fue exitoso por un largo periodo de tiempo.

En este caso se puede apreciar como el triángulo de fraude resalto en todo su apogeo. Según el criminólogo Donald Cressey, (citado por la Association of Certified Fraud Examiners, 2018a), el fraude tiene tres elementos principales:

1. Motivación
2. Oportunidad
3. Racionalización

Estos elementos integrándolos a nuestros perpetradores se puede exponer que fueron elaborados en todo su aspecto. Todos tuvieron la motivación para conspirar y llevar a cabo el esquema. Dentro de la oportunidad cuando comenzaron a investigar a sus víctimas consideraron cuales eran sus riesgos y se lanzaron a realizar el fraude. Y la racionalización es cuando nos percatamos que nadie hubiera simulado un estudiante graduado de maestría en fraude cometer un acto de tal magnitud. Como estudiante de sistema de seguridad en investigación de fraude, lo que pretendemos realizar es combatir estos crímenes para mantener una sociedad la cual no tenga que preocuparse por su seguridad en el ámbito tecnológico, sin embargo, comparando este objetivo con el que ellos realizaron es un tema controversial en la moral de un profesional.

SECCIÓN 6: AUDITORÍA Y PREVENCIÓN

En esta sección se estarán señalando cuales fueron las fallas que ocasionaron que los perpetradores tuvieran un acceso fácil para que el delito de fraude por medio de correo electrónico tuviera éxito por un límite de tiempo dentro de la compañía. La auditoría se basa en analizar los riesgos que pueden suceder en una organización la cual permita proveer una garantía de que la tecnología de información y los procesos en una organización están bajo un control de evaluación el cual puedan ser procesados de manera confiable.

Según Gutierrez-González (2016), la gerencia de una organización o empresa necesita establecer herramientas de controles internos estratégicos para lograr el cumplimiento de sus metas y objetivos establecidos, los cuales deben ser cónsonos con la visión y misión de la entidad. El auditor interno en sus funciones siempre debe estar vigilante para identificar y evaluar la vulnerabilidad del sistema de control en aquellas actividades que conlleven riesgo en la entidad. Mediante evaluaciones continuas los auditores internos pueden identificar el estado de efectividad de los procesos de riesgo y control interno.

Dentro de este caso observamos como los perpetradores lograron obtener información de las compañías para poder accesar a correos electrónicos que fueran similares a los altos gerenciales. El primer riesgo que vemos aquí es cuando las victimas contestan los correos electrónicos y no se percatan de la confiabilidad de este. En las empresas es esencial que posean un alto nivel de seguridad en su sistema tecnológico debido a la gran información que estos poseen, la cual los convierte en un punto estratégico para que sean víctimas de distintos tipos de fraude. Los mismos deben poseer siempre un antivirus que esté vigente junto con un firewall, el cual se hará responsable de no permitir acceso a hackers que deseen entrar en la computadora

para tomar el control de esta y realizar ataques para robar datos confidenciales que se encuentren en el disco duro.

Por otro lado, los correos electrónicos fueron realizados bajo la modalidad de *spoofing* lo cual es importante que las empresas tengan algún software que identifique cuando este riesgo esté sucediendo y automáticamente realice una señal la cual notifique que hay algo sospechoso ocurriendo. Según Trend Micro (2018) el programa Trend Micro Email Security, impulsado por XGen, utiliza una combinación de tecnologías intergeneracionales para ayudarlo a proteger, detectar y responder a los ataques de correo electrónico de *phishing* y *malware*. Estas soluciones de correo electrónico funcionan con *Control Manager* para una gestión centralizada además de compartir amenazas con otras capas de seguridad para mejorar la visibilidad y protección general. El programa utiliza progresivamente técnicas más avanzadas para un análisis preciso con un mínimo de demoras en la entrega de correo legítimo.

Estas técnicas son las siguientes:

1. Captura los ataques BEC utilizando inteligencia artificial, incluido un sistema experto y aprendizaje automático, para examinar el encabezado del correo electrónico, el contenido y autoría, y aplica una protección más estricta para los usuarios de alto perfil.
2. Evita las estafas ejecutivas de suplantación de identidad utilizando una exclusiva tecnología de DNA de estilo de escritura.
3. Comprueba el estilo de escritura de un correo electrónico entrante en inglés afirmó ser de un ejecutivo en contra de un modelo de aprendizaje automático entrenado de la escritura de ese ejecutivo.

4. Las únicas soluciones de seguridad de correo electrónico con aprendizaje automático previo a la ejecución para encontrar con precisión programas maliciosos desconocidos sin demoras.
5. El análisis que detecta amenazas desconocidas adicionales en los archivos adjuntos de correo electrónico, que incluyen: Documentos de Office, PDF, Archivos, ejecutables, scripts y multimedia.
6. Realiza análisis de URL tanto durante el tránsito como en tiempo real cuando un usuario hace clic en un enlace. Analiza las direcciones URL dentro de los archivos adjuntos de correo electrónico y scripts.

Otro asunto que debe mantener un control de seguridad es cuando el correo electrónico es contestado por la víctima y que la misma realice todos los pasos que dicta el correo sin verificar la información expuesta para mantener una autenticidad de la misma, ya sean cuentas bancarias extranjeras que los empresarios tengan para así poder proceder con la transferencia que se le está exigiendo y solicitar una autorización de un empleado de mayor jerarquía para aprobación y verificación o llamar a la persona que lo solicita para corroborar la misma.

Por medio de este análisis es importante que la compañía tenga unos controles de seguridad rigurosos los cuales ayuden a que estos eventos no ocurran en futuras ocasiones ya que existen muchas metodologías para acceso a información personal, privada la cual son utilizadas para realizar cualquier propósito ilícito. Dentro de la recomendación al programa Trend Micro existen diversos los cuales ayudan a combatir esta modalidad de crimen la cual ha tomado un auge generando perdidas para muchas empresas a nivel mundial y es recomendable que las empresas posean un programa de tal magnitud para su seguridad e integridad en el ámbito laboral.

SECCIÓN 7: CONCLUSIÓN

Realizando este trabajo tuve la oportunidad de recopilar distinta información la cual me ayudo a realizar esta investigación. Dentro de la búsqueda del caso logre ver como hoy día existen distintas modalidades de fraudes electrónicos alrededor del mundo. Es sorprendente como la tecnología ha creado la facilidad a los perpetradores acceder a tanta información para que cometan sus hazañas. En este trabajo investigado acerca de los casos United States vs Adejumo, United States vs Odufuye, United States v Nwoke fue interesante ya que no tenía conocimientos acerca de la modalidad de fraude que los mismos realizaron. Los perpetradores utilizaron el fraude por medio de correos electrónicos haciéndose pasar por un CEO de la empresa con el propósito de obtener transferencias de dinero a cuentas manejadas por ellos.

Es sorprendente como los tres conspiraron de tal forma para crear este esquema por más de un año, robándose más de un millón de dólares de diversas compañías. En ámbitos de investigación es un fraude el cual debemos estar muy pendientes para poder atacarlo de manera efectiva. Esta modalidad ha tenido un gran auge en los pasados años debido a que la tecnología sigue avanzando y los perpetradores utilizan su creatividad para realizar tales atracos. Es por esto por lo que debemos mantener cautela con la información enviada por medio de la tecnología porque nunca sabemos cómo podría ser utilizada o como podría perjudicarnos ya sea a nosotros o un tercero. En fin, las empresas deben mantener su sistema totalmente actualizado y auditándolo cada cierto tiempo para que logren remediar los hallazgos que encuentren en el mismo para establecer controles que logren remediar el riesgo que podrían sufrir.

SECCIÓN 8: REFERENCIAS

Access Data. (2018). Forensic Toolkit (FTK). Recuperado de https://accessdata.com/products-services/forensic-toolkit-ftk

Agencies. (2018, junio 12). US arrests 30 Nigerians in crackdown on email scammers. Recuperado de https://www.today.ng/news/world/arrests-30-nigerians-crackdown-email-scammers-121798

Association of Certified Fraud Examiners. (2018a). Triángulo del Fraude. Recuperado de https://acfe-spain.com/recursos-contra-fraude/que-es-el-fraude/triangulo-del-fraude

Association of Certified Fraud Examiners. (2018b). What is Fraud?. Recuperado de https://www.acfe.com/fraud-101.aspx

FBI. (2017, febrero 27). Business E-Mail Compromise. Recuperado de https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Federal Bureau of Investigation. (2018, julio 12). Business E-mail Compromise The 12 Billion Dollar Scam. Recuperado de https://www.ic3.gov/media/2018/180712.aspx

Find Law. (2018). Wire Fraud. Recuperedo de https://criminal.findlaw.com/criminal-charges/wire-fraud.html

Gutierrez-González, M. A. (2016, diciembre 9*). El Auditor Interno: el Proceso de Riesgo y Control Interno Gerencial.* Recuperado de https://360bestpracticesmethodology.wordpress.com/2016/12/09/el-auditor-interno-el-proceso-de-riesgo-y-control-interno-gerencial/

Tatham, M. (2018, marzo 15). Identity Theft Statistics. Recuperado de https://www.experian.com/blogs/ask-experian/identity-theft-statistics/

Trend Micro (2018). Soluciones de seguridad para colaboración y correo electrónico. Recuperado de https://www.trendmicro.com/es_mx/business/products/user-protection/sps/email-and-collaboration.html

Trend Micro. (2016, enero 11). Security 101: Business Email Compromise (BEC) Schemes. Recuperado de https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes

United States Code. (n.d.). Recuperado de http://uscode.house.gov/

United States Department of Justice. (2018a, abril 20). Ohio Resident Admits Role in Business E-Mail Compromise Scheme. Recuperado de https://www.justice.gov/usao-ct/pr/ohio-resident-admits-role-business-e-mail-compromise-scheme

United States Department of Justice. (2018b, agosto 17). Ohio Resident Sentenced to 15 Months in Federal Prison for Role in Business E-Mail Compromise Scheme. Recuperado de

https://www.justice.gov/usao-ct/pr/ohio-resident-sentenced-15-months-federal-prison-role-business-e-mail-compromise-scheme

United States Department of Justice. (2018c, enero 3). Nigerian National Admits Role in Business E-Mail Compromise Scheme. Recuperado de https://www.justice.gov/usao-ct/pr/nigerian-national-admits-role-business-e-mail-compromise-scheme

United States Department of Justice. (2018d, marzo 12). Defendant Indicted in Brooklyn Federal Court for Transnational Cyber Scam. Recuperado de https://www.justice.gov/usao-edny/pr/defendant-indicted-brooklyn-federal-court-transnational-cyber-scam

United States Department of Justice. (2017, marzo 21). Lithuanian Man Arrested For Theft Of Over $100 Million In Fraudulent Email Compromise Scheme Against Multinational Internet Companies. Recuperado de https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme

United States Department of Justice. (2018e, septiembre 11). Nigerian Man Sentenced To 5 Years In Prison For Participating In Business Email Compromise Scams. Recuperado de https://www.justice.gov/usao-sdny/pr/nigerian-man-sentenced-5-years-prison-participating-business-email-compromise-scams

United States Department of Justice. (2018f, diciembre 12). Nigerian National Sentenced to 45 Months in Federal Prison for Role in Business E-Mail Compromise Scheme. Recuperado de https://www.justice.gov/usao-ct/pr/nigerian-national-sentenced-45-months-federal-prison-role-business-e-mail-compromise

United States v. Adejumo, 3:18-cr-00082 (United State District Court District of Connecticut 2018).

United States v. Odufuye, 3:16-cr-00232 (United State District Court District of Connecticut 2018).

Wootson, C. R. (12 de junio de 2018). It’s time to stop laughing at Nigerian scammers because they’re stealing billions of dollars. *The Washington Post*. Recuperado de https://www.washingtonpost.com/news/business/wp/2018/06/12/its-time-to-stop-laughing-at-nigerian-scammers-because-theyre-stealing-billions-of-dollars/?noredirect=on&utm_term=.a7bc54736334