**EDP UNIVERSITY OF PUERTO RICO, INC.**

**RECINTO DE HATO REY**

**PROGRAMA DE MAESTRIA EN SISTEMAS DE INFORMACIÓN**

**Especialidad en Seguridad de Información e Investigación de Fraude**

**ROBO DE BITCOIN (DARKWEB)**

**(USA Vs.  MICHAEL RICHO)**

Caso Número: 3:16−mj−00464−JGM−1

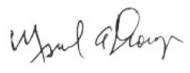
REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Especialidad en Seguridad de Información e Investigación de Fraude

PREPARADO POR:

MILITZA CASIANO BELTRAN

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



ANALISIS CASO DE FRAUDE ELECTRONICO EN ESTADOS UNIDOS DE AMERICA

(USA V. MICHAEL RICHO)

Numero de Caso: 3:16-mj-00464-JGM

Preparado por: Militza Casiano Beltrán

Ha sido aceptado como requisito parcial para el grado de: Maestría en Sistema de Información:

Especialidad en Seguridad Informática y Fraude

Julio, 2018

Aprobado por:

Dr. Miguel A. Drouyn Marrero, Director

**DEDICATORIA**

Agradecida por haber cumplido una meta más en mi vida. Quisiera dedicarles este escrito a mis padres, Santos Casiano y Gloria Beltrán, por su continuo apoyo a todas las metas que me propongo en la vida. Los adoro con todo mi corazón. También, a mi hijo y novio que tuvieron la paciencia de lidiar conmigo en mis momentos de estrés.

A mis compañeros de EDP University y ahora grandes amigos, siempre me brindaron su apoyo y consejos durante toda la maestría. Feliz de haber conocidos unas personas tan especiales.

Mis compañeros de trabajo que también me brindaron su apoyo y conocimiento con las dudas que se me ocurrían. Muy agradecida.

Mis profesores, Dr. Drouyn, Prof. De Diego, Prof. Ruiz, y Prof. Nelluid y todos los que me brindaron su ayuda y conocimiento del material de cada clase.

Muchísimas gracias a todos los que mencionó en este escrito, no fueron momentos fáciles, ya que casi terminando la maestría, pasó un huracán categoría cinco. Tener que estudiar sin luz no fue nada cómodo, pero lo logré. Orgullosa de mí por haber completado esta maestría.

**TABLA DE CONTENIDO**

**SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO**  1

Introducción 1

Descripción del caso 5

Trasfondo del caso 6

Descripción de los hechos 6

Acusaciones – Cargos – Penalidad 9

Definición de términos 9

**SECCIÓN 2: REVISIÓN DE LITERATURA**  12

Introducción 12

Fraudes involucrados 12

Leyes aplicables 16

Casos relacionados 19

Herramientas de investigación 21

**SECCIÓN 3: SIMULACIÓN**  22

**SECCIÓN 4: INFORME DEL CASO**  25

Resumen Ejecutivo 25

Objetivo 25

Alcance del Trabajo 25 Datos del Caso 26

Descripción de los Dispositivos Utilizados 26

Resumen de Hallazgos 26

Cadena de Custodia 27

Procedimiento 29

Conclusión 33

**SECCIÓN 5: DISCUSIÓN DEL CASO**  35

**SECCIÓN 6: AUDITORIA Y PREVENCIÓN**  36

**SECCIÓN 7: CONCLUSIÓN**  38

**SECCIÓN 8: REFERENCIAS**  39

**TABLA DE CONTENIDO**

**FIGURA 1:**  Entidades que reciben Ataques de *phishing* 13

**FIGURA 2**: Por ciento de los países atacados por *phishing* 16

**FIGURA 3:** *Phishing* del acusado 23

**FIGURA 4:** Trasferencia de los “Bitcoins” 24

**FIGURA 5**: Caso creado en OSForensic 30

**FIGURA 6:** Evidencia del texto encontrada en el disco duro 31

**FIGURA 7**: El contexto del nicefancy0929.txt 32

**FIGURA 8:** Evidencia de la conversación 33

**Seccion 1: Introducción y Trasfondo**

**Introducción**

Casos de fraude utilizando *bitcoin* se han convertido muy populares, ya que es difícil de rastrear. Según Horwitz (2018), *bitcoin* surge luego del año 2008, cuando un investigador anónimo publica un documento donde indica que puede resolver el asunto de centralización de las monedas no utilizando el banco. La persona lo llamó *bitcoin* y pasó hacer una solución descentralizada, es decir que no depende de un banco en particular.

Horwitz (2018) informa en su artículo, que las monedas *bitcoins* (o más bien las transacciones) se registran en un libro de contabilidad, este libro mayor es público y compartido. Igualmente lo mantiene el público. Miles de personas tienen una copia de este libro mayor por todo el mundo, y cualquiera puede descargar y verificarlo. En *bitcoin*, en lugar de cuentas, el dinero se mueve entre direcciones, tal como el correo electrónico.

Usualmente las personas les preocupan que el libro esté público, ya que no lo ven seguro, entiende que sería un problema con la seguridad. Lo ven fácil de *hackear*, pero imaginasen piratear la historia de la biblia católica, quizás puedan entrar a las bases de datos del Vaticano y cambiar la historia de la biblia, pero esto sería un problema. Hay muchas copias de la biblia en todo el mundo; no se pueden engañar a todos pirateando una sola copia. Lo que nos ayuda en el *bitcoin* permanecer en la misma página es el libro mayor que se llama *blockchain*. Todas las transacciones confirmadas están incluidas en el *blockchain*. De esta forma, los monederos de *bitcoin* pueden calcular su saldo gastable y se puede verificar que las nuevas transacciones estén. La integridad y el orden cronológico de la cadena de bloques se aplican con criptografía.

Según Horwitz (2018), una transacción es una transferencia de valor entre las carteras de *bitcoin* que se incluye en el *blockchain*. Las billeteras de *bitcoin* mantienen una pieza secreta de datos llamada clave privada o semilla, que se usa para firmar transacciones, proporcionando una prueba matemática de que provienen del propietario de la billetera. La firma también evita que la transacción sea alterada por alguien una vez que se haya emitido. Todas las transacciones se transmiten entre los usuarios y, por lo general, comienzan a confirmarse en la red en los siguientes 10 minutos, a través de un proceso llamado minería.

En el artículo escrito por Horwitz (2018), nos explica que la minería es un sistema de consenso distribuido que se utiliza para confirmar las transacciones en espera al incluirlas en la cadena de bloques. Hace cumplir un orden cronológico en el *blockchain*, protege la neutralidad de la red y permite que diferentes computadoras acuerden el estado del sistema. Para confirmar, las transacciones se deben empaquetar en un bloque que se ajuste a reglas criptográficas muy estrictas que serán verificadas por la red. Estas reglas evitan que los bloques anteriores se modifiquen porque al hacerlo invalidaría todos los bloques siguientes. La minería también crea el equivalente de una lotería competitiva que evita que cualquier individuo agregue fácilmente bloques nuevos de manera consecutiva en la *blockchain*. De esta forma, ningún individuo puede controlar lo que está incluido en la cadena de bloques o reemplazar partes de la cadena de bloques para reducir sus propios gastos.

¿Cómo *bitcoin* cambiaría el mundo? *Bitcoin* no es geográfico. Según Horwitz (2018), si el gobierno cambia o las economías caen, *bitcoin* no se verá afectado como el dólar u otras monedas. Es amigable con el internet, lo que sería muy beneficioso para los comercios en línea.

Expliqué cómo funciona *bitcoin* y algunos de los beneficios del mismo. Ahora les hablo de las desventajas del *bitcoin*. Según Horwitz (2018), la mayor desventaja del *bitcoin* son los riesgos de seguridad. El *bitcoin* es prácticamente imposible duplicar, pero esto no significa que sean inmunes al robo o al fraude. *Bitcoin* tiene sus puntos débiles y atractivos para los *hackers*. El bitcoin al no ser independiente políticamente y fuerte protecciones anónimas, eso lo hace atractivo para ladrones y estafadores. A las autoridades se les hace difícil enjuiciar a los responsables de los atracos de *bitcoin*, muchos que se producen en naciones políticamente débiles o poco amistosas. Los mercados web oscuros (mercados negros internacionales en línea cuyos usuarios compran y venden sustancias ilícitas, bienes robados y servicios prohibidos) son objetivos frecuentes de atraco. Es probable que los usuarios de *bitcoin* que participan en la web oscura ya infrinjan la ley.

Adelante menciono los métodos comunes de robo de Bitcoin:

* Billeteras Falsas – Según Madeira (2017), este método es mucho menos popular, pero ha estafado exitosamente a los usuarios desconocidos de sus monedas. Las billeteras falsas son básicamente aplicaciones que inicialmente parecen una billetera real hasta que tienen la oportunidad de robar sus monedas. Estas carteras falsas generalmente son respaldadas como otra billetera legítima, a menudo usando el logotipo y el nombre de la billetera real para engañar a los usuarios. Básicamente son como el phishing para billeteras en lugar de sitios web o correos electrónicos.
* *Bitcoin Phishing:* Como indica Madeira (2017), el phishing es básicamente un medio para extraer información sensible de las víctimas. Existen variaciones en el esquema, pero las más comunes son correos electrónicos y sitios web falsos. Los estafadores intentarán engañar a la víctima para que le brinde información confidencial sobre sus Bitcoins, como los datos de inicio de sesión de un intercambio o una billetera en línea.
* Esquema *Ponzi:* Según Madeira (2017), *bitcoin* y otras criptomonedas están llenas de esquemas populares de Ponzi, también conocidos como esquemas de pirámides. Esto implica que las personas inviertan dinero e inviten a más personas a invertir dinero, creando así el efecto de la pirámide. El dinero nuevo se usa para pagar inversiones antiguas y "la rueda sigue girando" hasta que ya no pueda volverse. Llega un punto que el estafador se irá con el dinero de todos.

Según USA vs. Michael Richo (2016), el *dar web* y *tor*, que es un acrónimo de *The Onion Router*, es una red especial de computadoras en internet, distribuidas por todo el mundo, diseñadas para ocultar las verdaderas direcciones IP de las computadoras en la red, y, por lo tanto, las identidades de los usuarios de la red. Cada comunicación enviada a través de *tor* se rebota a través de numerosos relevos dentro de la red, y envuelto en numerosas capas de cifrado, de modo que es prácticamente imposible rastrear comunicación de regreso a su verdadera dirección IP de origen. *Tor* también permite que los sitios web funcionen en la red de una manera que oculta las direcciones IP verdaderas de los servidores de la computadora que alojan los sitios web. Tales "servicios ocultos" que operan en *tor* tienen direcciones web complejas, generadas por un algoritmo informático, que termina en *onion* (en lugar de .*com* o .*net*). Para acceder a la red *tor,* puedes simplemente descargar el *software* del navegador *tor* y usarlo para acceder al *internet*. Debido al anonimato proporcionado a los usuarios y sitios web en la red *tor*, a veces conocida como la web oscura.

Muchos criminales se aprovechan del web oscuro para hacer cosas ilegales. Como Michael Richo, 35, la cual se involucró en un esquema de *phishing* para robar *bitcoins* de individuos en la web oscura. Se estima que se robó alrededor de 365,000 en *bitcoins.*

**Descripción del Caso**

Numero de Caso: 3:16−mj−00464−JGM−1

Partes del Caso: Estados Unidos Vs. Michael Richo

Acusado: Michael Richo

Investigador: Special Agent Michael Morrison, Federal Bureau of Investigation (FBI)

Abogados: Lic. Tracey Hayes

Juez: Hon. Sarah A.L. Merriam, United States Magistrate Judge, District of Connecticut

**Transfondo**

Michael Richo, 35, de Wallingfort, Connecticut, se dedicaba a hackear y entrar a mercados web oscuros. La técnica de fraude que utilizó Richo fue *phishing*, su conocimiento en programación le ayudó a engañar a miles de personas. Tiene conocimiento de experto en *exploit*, *scanning, rooting boxes, backdoors* y sobre la construcción de un *botnet* de computadora con *Windows*.

**Descripción de Hechos**

Según USA vs. Michael Richo (2016), el FBI comenzó a investigar a Richo en noviembre del 2013 con relación a su implicación al mercado negro, donde se especializa vender drogas, tarjetas robadas y otros artículos ilícitos. El FBI obtuvo información de que el acusado podía estar involucrado en un esquema de *phishing* donde lograba conseguir nombres de usuarios y contraseñas para poder robarles sus *bitcoins*. Al momento de lo sucedió el acusado residía en West Haven, Connecticut.

Como indica USA vs. Michael Richo (2016), el 4 de noviembre del 2014, la jueza Hon. Fitzsimmons, emitió una orden de búsqueda e incautación para la residencia del acusado en West Haven. Durante la incautación los agentes del FBI encontraron varias computadoras, disco duros externos, y memoria USB. Durante la búsqueda el acusado cedió a una entrevista con los agentes donde admite lo siguiente:

* Tenía un negocio llamado *MediaPen*.
* Robaba *bitcoins* a los usuarios y proveedores que intentaban acceder al mercado en línea *tor network* mejor conocido como el mercado negro.
* Utilizó dos métodos de estafa para poder robar información confidencial de los usuarios:

1. Publicaba enlaces falsos en los foros del mercado negro que redirigirían a los usuarios a un inicio de sesión falsa. La página de inicio de sesión se vería exactamente como las páginas de inicio de sesión real para los diversos sitios del mercado negro. Cuando los usuarios intentan iniciar sesión, él robaba sus nombres de usuario y contraseñas.
2. La otra técnica utilizada por el acusado para robar credenciales de acceso implicaba publicar enlaces falsos en foros que, al hacer clic, redirigían a los usuarios a través del servidor de la computadora del acusado al sitio real del mercado donde los usuarios iniciarían sesión. El acusado registraría todo el tráfico de los usuarios incluyendo su información confidencial.

* Una vez que el acusado tuviera acceso a la cuenta de un usuario, usaría un programa llamado *bitcoin monitor* para que le notificará cuando se realizó un depósito en la billetera *bitcoin* del usuario. Después al recibir la notificación de un depósito, se registraba (usando las credenciales del usuario) en la cuenta y retiraba los *bitcoins* antes que el usuario los gastará. A menudo usaba *bitcoin fog*, cuando transfería los *bitcoins* para ocultar su rastro. Los *bitcoins* serían depositados en su billetera utilizando *local bitcoins*, donde los vendería a cambio de depósitos en efectivo y los transfería a su cuenta de Bank of America. Nombre de usuario del acusado en *local bitcoins* fue *bmerc*.
* El acusado calculó que había robado más seis cifras de *bitcoins*.
* El acusado declaró que tenía un programa en su computadora portátil que almacenaba los usuarios y contraseñas en un archivo llamado "*nicefancy.txt*". El acusado creía que actualmente había terminado en 10,000 líneas de texto.

Durante la entrevista, el acusado también aconsejó a los agentes del FBI que tenía unidades adicionales de computadora en una caja de depósito de seguridad en *People's United Bank*. El FBI visitó *People's United Bank* y confiscó el contenido de la caja de depósito de seguridad del acusado, que contenía, entre otras cosas, un disco duro y memorias USB.

Según USA vs. Michael Richo (2016), el FBI obtuvo las cuentas de banco de la compañía *MediaPenLLC* en el *Bank of America* y observó numerosos depósitos de moneda estadounidense, algunos de los cuales corresponden a las ventas de *bitcoins*, algunos ejemplos de los que se encontraron los agentes del FBI son:

* El 5 de noviembre de 2013, hubo dos transacciones de venta de *bitcoins* en *Local*

*Bitcoins* por $ 350 y $ 340. Ese mismo día, hubo dos depósitos en el *Bank of America* cuenta por $ 350 y $ 340 con la descripción *counter de credit*.

* El 8 de noviembre de 2013, hubo cuatro transacciones de venta de *bitcoins* en *local bitcoins* por $ 200, $ 350, $ 999.88 y $ 1,000. Ese mismo día, hubo cuatro depósitos en el *Bank of America* de *Mediapen* cuenta con $ 200, $ 350, $ 999.88 y $ 1,000 con la descripción *counter* *credit*.
* El 9 de noviembre de 2013, hubo una transacción de venta de *bitcoins* en *local* *bitcoins* por $ 378. El 12 de noviembre de 2013, hubo un depósito en el *Bank of America* cuenta por $ 378 con la descripción *counter credit*.
* El 12 de noviembre de 2013, hubo una transacción de venta de *bitcoins* en *local*

*bitcoins* por $ 801. Ese mismo día, hubo un depósito en el *Bank of America* de *Mediapen* cuenta por $ 801 con la descripción "contador de crédito".

En total, de noviembre de 2013 a octubre de 2014, hubo más de $ 100,000 en efectivo

depósitos en la cuenta de *Bank of America* de *Mediapen*, la mayoría tiene la descripción "contador crédito."

Michael Richo, que fue arrestado el 5 de octubre de 2016, se robó un total de $ 365,000 en *bitcoins* de los mercados de *darknet.*

**Acusaciones, Cargos y Penalidades**

Se presentaron cinco acusaciones contra el acusado por haber violado el titulo 18 del código de Estados Unidos, las secciones 1029(a)(2),1029(a)(3), 1030(a)(2), 1030(a)(4), 1343, 1028A, 1956.

1. 1029(a)(2) y (a)(3) - Acceso al fraude del dispositivo
2. 1030(a)(2) y (a)(4) - Fraude informático
3. 1349 - Fraude alámbrico
4. 1028A - Robo de identidad agravado
5. 1956(a)(1)(B)(i) – Lavado de dinero

**Definiciones y Términos**

Las siguientes definiciones provienen de Wikipedia (s.f.)

**Bitcoins**: es una criptomoneda, una forma de efectivo electrónico. Fue diseñado para funcionar como una moneda digital descentralizada sin un banco central o administrador único.

**Bitcoin Fog**: es un “cryptocurrency tumbler” centralizado para bitcoin.

**Cryptocurrency Tumbler**: es un servicio ofrecido para mezclar los fondos de criptomoneda potencialmente identificables o 'contaminados' con otros, a fin de ocultar el rastro a la fuente original del fondo. Los vasos han surgido para mejorar el anonimato de las criptomonedas, generalmente bitcoin (por lo tanto, mezclador Bitcoin), ya que las monedas proporcionan un libro público de todas las transacciones.

**Local Bitcoin**: es una empresa startup de bitcoin con sede en Helsinki, Finlandia. Su servicio facilita la negociación extrabursátil de moneda local para bitcoins. Los usuarios publican anuncios en el sitio web, donde establecen las tasas de cambio y los métodos de pago para comprar o vender bitcoins.

**Blockchain**: originalmente cadena de bloques, es una lista creciente de registros, llamados bloques, que se vinculan mediante criptografía. Las criptomonedas utilizan ampliamente las cadenas cuadradas que son legibles por el público

**Phishing**: es el intento fraudulento de obtener información confidencial como nombres de usuario, contraseñas y detalles de la tarjeta de crédito (y dinero), a menudo por razones maliciosas, disfrazándose como una entidad confiable en una comunicación electrónica

**Exploit**: es una pieza de software, un fragmento de datos o una secuencia de comandos que aprovecha un error o una vulnerabilidad para provocar un comportamiento involuntario o imprevisto en un software, hardware o algo electrónico (generalmente computarizado)

**Rooting:** es el proceso que permite a los usuarios de teléfonos inteligentes, tabletas y otros dispositivos que ejecutan el sistema operativo móvil Android obtener un control privilegiado (conocido como acceso raíz) en varios subsistemas de Android.

**Backdoors**: es un método, a menudo secreto, de eludir la autenticación o el cifrado normal en un sistema informático, un producto o un dispositivo integrado (por ejemplo, un enrutador doméstico) o su realización, como parte de un criptosistema, un algoritmo, un chipset o una " homunculus computer ", una pequeña computadora dentro de una computadora (como la que se encuentra en la tecnología AMT de Intel).

**Bot**: es una aplicación de software que ejecuta tareas automáticas (scripts) a través de Internet. Típicamente, los bots realizan tareas simples y estructuralmente repetitivas, a una velocidad mucho mayor de la que sería posible para un humano solo.

**Botnet**: es una cantidad de dispositivos conectados a Internet, cada uno de los cuales ejecuta uno o más bots. Las botnets pueden usarse para realizar un ataque de denegación de servicio distribuido (ataque DDoS), robar datos, enviar spam y permite al atacante acceder al dispositivo y su conexión.

**Seccion 2: Revision de Literatura**

**Introducción**

Muchos de los hackers utilizan la web oscura como medio de cometer fraude, robos, vender drogas, ect. Los agentes de FBI están encargados de atrapar a estos hackers y hacer que paguen por los robos. Se han encargado de desarrollar nuevas técnicas, y probable desarrollen aún más formas de atrapar a los delincuentes expertos en la tecnología.

**Fraudes Involucrados**

El *phishing* afectado cada día más a las empresas financiera y salud, entre otras. Según Vadeolmillos (2018), los ciberataques a las empresas adoptan muchas formas y llegan por medios muy diversos. Uno de ellos es el correo electrónico. Es por tal razón que las empresas tanto grandes como pequeñas deben estar en alerta de estos ataques, que se ha vuelto muy común. Tanto, que el 90% de las empresas ha visto un aumento en el volumen de ataques de *phishing*.

Según Valdeolmillos (2018), una investigación que fue elaborada por la empresa MCPRO, se hizo una encuesta a 800 directivos y responsables de tecnología de varias compañías. Según el informe se concluyó que los ciberataques han aumentado en todo el mundo. Cerca del 50% de las empresas aseguran que el volumen de los ataques de phishing ha subido en el último año. Además, el 40% ha destacado que los ataques que se inician mediante mensajes que simulan ser de otra persona.

Como indica Valdeolmillos (2018), los ataques están afectando a la planilla como también a los directivos de las empresas. Y los resultados que obtuvo la empresa MCPRO vieron que no siempre estos cuentan con la mejor preparación para evitarlos. Así se desprende de las respuestas recogidas en la encuesta.

Según Valdeolmillos (2018), los directivos de las empresas, para las que trabajan el 20% de los encuestados aseguran que sus directivos de primer nivel han enviado información importante en respuesta a un ataque de phishing. Además, el 49% admite que sus equipos de finanzas y gestión no cuentan con formación necesaria para identificar y detener un ataque de suplantación de identidad.

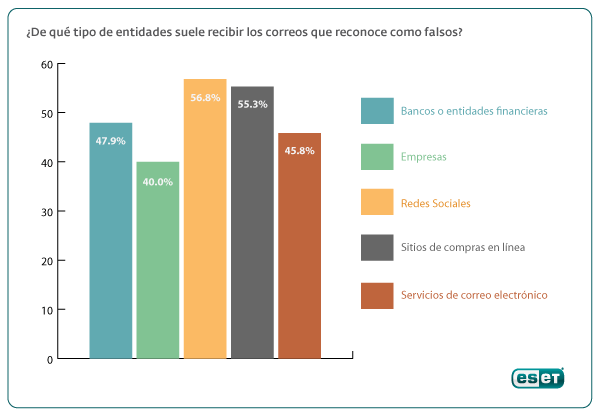


Figura 1: Entidades que reciben Ataques de Phishing (Tomado de https://habeasdatacpdp.wordpress.com/2011/02/22/phishing-ataques-y-realidades-2/)

Según Tecnósfera (2018), durante los primeros tres meses del 2018 hubo más de 3.7 millones de intentos de visitar páginas de redes sociales fraudulentas, de los cuales el 60 por ciento pertenecían a sitios falsos de la red social más usada, Facebook. Así lo revela el informe de Karpersky Lab ‘*Spam* y *Phishing* en el primer trimestre de 2018’.

Las redes sociales es la herramienta más común por los atacantes no solo para difundir a través de ellas las estafas sino también para suplantarlas. Según Tecnósfera (2018), el estudio señala que los atacantes falsifican continuamente la página de Facebook para tratar de robar datos personales utilizando la técnica de *phishing*. Según el reporte los ciberdelincuentes tienen como objetivo obtener información como los nombre, la contraseña o el número de tarjeta de crédito.

Como indica Tecnósfera (2018), Nadezhda Demidova, analista principal de contenido web para Kaspersky Lab, resalta que a pesar de los recientes escándalos globales sobre filtración de datos, "las personas continúan haciendo clic en enlaces inseguros y dan permiso a aplicaciones desconocidas para que accedan a su información personal. Debido a esta falta de vigilancia del usuario, los datos de una gran cantidad de cuentas se pierden o son usados para extorsionar a los usuarios. Esto puede conducir a ataques y un flujo constante de dinero para los ciberdelincuentes”.

Según Tecnósfera (2018), cibercriminales lograron obtener cerca de 35,000 dólares a través de un sitio falso que ofrecía supuestamente la oportunidad de invertir en Telegrama ICO, la plataforma de *blockchain* del servicio de mensajería.

Como indica Tecnósfera (2018), los atacantes también han aprovechado la coyuntura de la entrada en vigencia del Reglamento general para la protección de datos en Europa, GDPR por sus siglas en inglés, para enviar correos electrónicos con enlaces falsos que incluyen supuestas ofertas de *webinars* (seminarios en la web) para aclarar la nueva legislación o invitaciones para instalar un software especial que proporcionará acceso a recursos en línea, según informa Kaspersky.

Aunque las redes sociales han sido atacadas, el *phishing* financiero continúa representando casi la mitad de todos los ataques de esta modalidad. Los 3 principales ataques para estafar son contra los siguientes:

* Bancos
* Tiendas electrónicas
* Los sistema de pago

Figura 2: Por ciento de los países atacados por phishing (Tomado de: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/casos-de-phishing-en-redes-sociales-en-2018-224936)

**Leyes Aplicables**

Las leyes violadas en el caso de United States of America vs. Michael Richo son las siguientes:

* Titulo 18 del Codigo de Estados Unidos, Seccion 1029(a)(2) - prohíbe a una persona a sabiendas y con la intención de defraudar, utilizando uno o más dispositivos de acceso no autorizados durante cualquier período de un año y por tal conducta, obteniendo cualquier cosa de valor que agregue $ 1,000 o más durante ese período. 18 U.S.C. §I 029 (a) (3) prohíbe además que una persona intencionalmente, y con la intención de defraudar, posea quince o más dispositivos de acceso no autorizados. El término "dispositivo de acceso" se define para significar, entre otras cosas, cualquier tarjeta, número de cuenta, número de serie electrónico, número de identificación personal, u otro medio de acceso a la cuenta que se puede usar, solo o junto con otro acceso dispositivo, para obtener dinero, bienes, servicios o cualquier otra cosa de valor, o que se puede utilizar para iniciar una transferencia de fondos. El término "dispositivo de acceso no autorizado" se define como cualquier dispositivo de acceso es decir, entre otras cosas, robado o caducado con la intención de defraudar.
* Título del Codigo de Estados Unidos, Seccion 1343 - (fraude informático) prohíbe a una persona, entre otros cosas, acceder a una computadora sin autorización y, por lo tanto, obtener información de un computadora protegida 18 U.S.C. § 1 030 (a) (4) además prohíbe a una persona a sabiendas y con intento de defraudar, acceder a una computadora protegida sin autorización, y por medio de llevar a cabo el fraude pretendido y obtener cualquier cosa de valor, a menos que el objeto del fraude y lo que se obtiene consiste solo en el uso de la computadora y el valor de dicho uso es no más de $ 5,000 en cualquier período de un año. El término "computadora protegida" se define para incluir, entre otras cosas, una computadora utilizada o que afecta el comercio o la comunicación interestatal o extranjera
* Título del Código de Estados Unidos, Sección 1028A - (fraude electrónico) prohíbe a una persona que, habiendo ideado o tiene la intención idear cualquier esquema o artificio para defraudar, o para obtener dinero o propiedad mediante falsos o pretensiones, representaciones o promesas fraudulentas, transmite o hace que se transmita por medios de cable, en el comercio interestatal o extranjero, cualquier escritura, señalización, señal, imagen o sonido con el propósito de ejecutar tal esquema o artificio.
* Título del Código de Estados Unidos, Sección 1956(a)(1)(B)(i) - (robo de identidad agravado) prohíbe a una persona, durante y en relación con ciertos crímenes enumerados, desde transferir, poseer o usar a sabiendas, sin autoridad legal, un medio de identificación de otra persona. Los felonías enumerados incluyen cualquier violación de los Capítulos 47 y 63, que, a su vez, incluye violaciones de 18 U.S.C. §§ 1029 (fraude de dispositivos de acceso), 1030 (fraude informático) y 1343 (fraude electrónico). El término "medio de identificación "se define para incluir, entre otras cosas, cualquier nombre o número que pueda usarse, solo o en conjunto con cualquier otra información, para identificar a un individuo específico, incluyendo, entre otras cosas, un nombre, número de seguro social o número o dirección de identificación electrónica única. El término "medio de identificación" también incluye un "dispositivo de acceso" como se define en 18 u.s.c. § 1029.

**Casos Relacionados**

El caso de Michael Richo no es el único con esquema de *phishing*. Durante el 2018 ha subido el porciento de ataques a los usuarios para poder acceder a datos, esa información es muchas veces vendida en la *dark web*. Además, de atacar a las empresas y exigirles un pago para poder liberar la información que tienen de sus sistemas, los hackers solicitan los pagos en *bitcoins*. El FBI ha estado trabajando fuerte para poder atrapar a estos criminales. En el 2018 un total de 74 personas fueron arrestadas en varios territorios, incluidos EE. UU. Y Nigeria, y la mayoría de los arrestados fueron acusados ​​de participar en una estafa de compromiso comercial por correo electrónico.

United States of America v. Olajide Abraham Eyitayo 2018 – Este caso con el numero 1:17-cr-269, involucra un hombre que fue sentenciado a prisión por estafa de “phishing” por correo electrónico de $ 1.1 millones. Olajide Abraham Eyitayo, de 46 años, de Hempstead, abrió tres cuentas bancarias en enero de 2016 utilizando una empresa que formó en Nueva York. De enero a abril de 2016, las cuentas estuvieron esencialmente inactivas, y al 25 de abril de 2016, los saldos combinados de las tres cuentas eran de menos de cinco dólares. Ese día, una asociación comercial con sede en Virginia aprobó un pago de más de $ 280,000 destinado a un proveedor de viajes, pero el pago fue a una de las cuentas de Eyitayo. La asociación había cambiado la información de pago del proveedor el mes anterior, cuando un correo "falso" que suplantaba al proveedor solicitaba que la información de pago se cambiara al número de cuenta que pertenecía a Eyitayo. Durante los siguientes meses, Eyitayo recibió dos pagos más en su cuenta destinado al proveedor de viajes de la asociación. En total, Eyitayo recibió más de $ 1.1 millones en ganancias fraudulentas.

United States of America v. Konrads Voits – Este caso con el numero 2:17-cr-20689-RHC-MKM, involucra un hombre que fue sentenciado a prisión idear y ejecutar un plan para acceder y causar daños al sistema informático del gobierno del Condado de Washtenaw. De acuerdo con los registros judiciales, Voits ejecutó un esquema clásico de "phishing", donde Voits usaba tanto correos electrónicos como llamadas telefónicas a los empleados del condado de Washtenaw, para finalmente obtener acceso y control de la red informática del condado de Washtenaw. Al obtener acceso, Voits tomó los nombres, direcciones, correos electrónicos y contraseñas de muchos empleados anteriores y actuales del Condado de Washtenaw. Además, Voits accedió a los registros de la cárcel del condado de Washtenaw, alterando los registros electrónicos de al menos un preso en un esfuerzo por liberar a ese preso antes de tiempo. Gracias a una cuidadosa revisión por parte de los empleados de la cárcel del condado de Washtenaw, ningún recluso fue liberado temprano. El condado de Washtenaw gastó miles de dólares y numerosas horas de trabajo adicionales para responder e investigar la infracción, lo que resultó en una pérdida de al menos $ 235,488.

## United States of America v. Karim Baratov, a/k/a “Kay,” a/k/a/Karim Taloverov, a/k/a Karim Akehmet Tokbergenov- Este caso con el numero 3:17-cr-00103-VC, involucra un hacker canadiense que conspiraró con y ayudó a oficiales rusos del FSB, se declara culpable. El FSB ordenó un hacker prolífico para dirigirse a cuentas de correo web en nombre del gobierno ruso. Baratov, de 22 años, ciudadano canadiense y residente, y otros tres acusados, incluidos dos oficiales del Servicio Federal de Seguridad de Rusia ("FSB"), el servicio de inteligencia y aplicación de la ley nacional de Rusia, fueron acusados ​​de piratería informática y otros delitos en conexión con una conspiración para acceder a la red de Yahoo y los contenidos de las cuentas de correo web que comenzaron en enero de 2014. Los codemandados de Baratov, todos los cuales permanecen prófugos en Rusia, todos son ciudadanos y residentes rusos: Dmitry Aleksandrovich Dokuchaev, de 33; Igor Anatolyevich Sushchin, 43; y Alexsey Alexseyevich Belan, a / k / a "Magg", 29.

**Seccion 3: SimulacióN**

Según el pliego acusatorio United States of America vs. Michael Richo el fraude cometido ocurrió de la siguiente manera:

1. El acusado tenía dos maneras de robar las credenciales a los usuarios y proveedores que intentaban entrar al mercado a la red *tor*.
2. Primer método que utilizaba para robar las credenciales era posteando enlaces falsos en los foros del mercado negro, estos enlaces dirigían a los usuarios hacer iniciación a una página web, la cual era dirigida por el acusado. La página web de iniciación era idéntica a la página real de varios sitios del mercado donde los usuarios harían su iniciación. Cuando los usuarios intentaban entrar con sus credenciales a la página web, el acusado se robaba sus contraseñas y nombres de usuarios.
3. Otro método que utilizaba el acusado fue posteando enlaces falsos en foros del mercado negro, tan pronto el usuario le daba clic, los redirigía por la computadora del acusado al servidor actual de los sitios del mercado, ahí los usuarios se registran en la página con sus credenciales y el acusado haría un *keylog* de todo el tráfico incluyendo la información de inicio del usuario.
4. El acusado tenía acceso a las cuentas de los usuarios, utilizaba un programa llamado *bitcoin monitor*. El programa le notificaba cuando el usuario hacia un depósito a su cartera de *bitcoin*, el acusado iniciaba a la cuenta del usuario y retiraba los *bitcoins* antes que el usuario los gastará. Usualmente usaba *Bit Fog* para la transferencia de *bitcoins*, usaba esa red para poder esconder su rastro. Cuando los *bitcoins* eran depositados a la cartera de *bitcoins* usando *local Bitcoins* donde los vendía a cambio de depósito en efectivo a su cuenta de Bank of America.
5. El acusado tenía un programa en su laptop que guardaba los usuarios y contraseñas en un archivo llamada *nicefancy.txt*. Tenía sobre 10,000 líneas de texto.

Figura 3: *Phishing* del acusado



Figura 4: Trasferencia de los “Bitcoins”

**Seccion 4: informe del caso**

Según los expedientes del caso de United States of America v. Michael Richo, se determinó contratar los servicios de MCB Forensics, un investigador forense digital, para trabajar con la evidencia entregada en la corte. El Agente del Federal Bureau of Investigation (FBI), Michael Morrison, entregó voluntariamente el disco duro.

La corte procede a permitir que se utilice el disco duro para extraer todo lo relacionado con el fraude ya que la corte lo catalogó como una colección de documentos electrónicos, pero a su vez, protegiendo y omitiendo todo archivo no relacionado al caso. El disco duro contiene varios archivos en texto y conversaciones electrónicas.

**Objetivo**

De acuerdo con los escenarios encontrados, los agentes del FBI y la Jueza de la corte han solicitado los servicios profesionales de MCB Forensic, Inc. El objetivo es analizar, descubrir y recuperar la información contenida en el disco duro relacionado al caso. La investigación se realiza con el propósito de obtener evidencia que ayude para que la corte pueda sostener un caso sólido y lograr la acusación del acusado del caso.

**Alcance del Trabajo**

Durante la fecha del 4 de octubre del 2016, la jueza Sara A. L. Merriam hacen entrega a la investigadora forense digital Militza Casiano, de la compañía MCB Forensics, el disco duro en donde puede existir la evidencia necesaria para poder ayudar a esclarecer el caso. El propósito es analizar el disco duro para buscar y tratar de hallar toda la información relevante y que sea útil en el caso. El investigador forense preparará un informe sobre los hallazgos encontrados en el disco duro con el propósito de entregar a la jueza toda la evidencia encontrada durante la investigación y ella pueda analizar, evaluar y utilizar como material para que tomo acción legal sobre el acusado.

**Datos del Caso**

1. Número del caso: 3:16-mj-00464-JGM
2. Caso: United States vs. Michael Richo
3. Investigador: Militza Casiano Beltrán
4. Cliente: Estados Unidos, Distrito Connecticut
5. Representante del cliente: Lic. Tracy Hayes y Jueza asignada Hon. Sarah A.L. Merriam

**Descripción de los Dispositivos Utilizados**

Los dispositivos utilizados durante este proceso son:

1. Laptop Dell Inspirion el cual contiene las herramientas forenses necesarias para la investigación.
2. OSForensics, Programa para realizar análisis forense digital
3. Disco duro externo Seagate Innov8 8TB

**Resumen de Hallazgos**

Durante el proceso del análisis de la evidencia, la investigadora forense realiza la adquisición, preservación, análisis, y presentación de la evidencia que se encontró en el disco duro. Es bien importante que todo sea manejado con mucha precaución lo entregado al investigador para evitar alteración, robo, perdida, o destrucción del material. De ocurrir algo de lo antes mencionando sería un daño para la investigación y el caso se podría caer. En la investigación se encontró evidencia que implica al acusado con los hechos de este caso. Existen archivos creados durante noviembre 2013 y noviembre 2014 con contraseñas y nombre de usuarios de las víctimas de robo de *bitcoins*. Además, se encontró conversaciones en línea. Lo que quiere decir que si el fraude fue cometido.

**Cadena de Custodia**

La cadena de custodia se diseñó con el propósito de que se realice el debido proceso de recopilar, analizar y almacenar la evidencia de forma correcta y en un orden de eventos para garantizar confiabilidad, confidencialidad e integridad y lograr así garantizar un proceso justo.

Luego de discutir los detalles de la cadena de custodia, se procede a detallar la cadena de custodia seguida por el investigador de la compañía MCB Forensics de este caso.

Primer evento:

* Descripción del evento: Evidencia recogida por la investigadora Sra. Militza Casiano Beltrán y entregada por la jueza Sara A. L. Merriam y la Lic. Tracy Hayes. La evidencia consiste en un disco duro externo Seagate Innov8 8TB.
* Evento verificado por: Militza Casiano Beltrán, Hon. Sara A.L. Merriam y la Lic. Tracy Hayes.
* Número de evidencia: E-1-2014-10-04.
* Fecha de comienzo: 14 de octubre de 2014 – 9:00 AM.
* Fecha de terminación: 14 de octubre de 2014 – 11:00 AM.
* Lugar de origen: Oficina del FBI.
* Lugar de destino: Laboratorio Forense MCB Forensics.

Segundo evento:

* Descripción del evento: Creación del número de caso y asignación de evidencia al mismo.
* Evento verificado por: Militza Casiano Beltran
* Número de evidencia: E-1-2014-10-04 asignado al caso # C-1-2014-10-04.
* Fecha de comienzo: 4 de octubre de 2014 – 4:30 PM.
* Fecha de terminación: 4 de octubre de 2014 – 7:00 PM.
* Lugar de origen: Laboratorio forense MCB Forensics
* Lugar de destino: Laboratorio Forense MCB Forensics

Tercer evento:

* Descripción del evento: Proceso de comenzar a analizar la evidencia para posteriormente realizar el informe para ser brindado a fiscalía.
* Evento verificado por: Militza Casiano Beltrán.
* Número de evidencia: E-1-2014-10-04 asignado al caso # C-1-2014-10-04.
* Fecha de comienzo: 5 de octubre de 2014 – 9:00 AM.
* Fecha de terminación: 5 de octubre de 2014 – 3:01 PM.
* Lugar de origen: Laboratorio Forense MCB Forensics
* Lugar de destino: Laboratorio Forense MCB Forensics

Cuarto evento:

* Descripción del evento: Entrega de informe de análisis forense directamente a la jueza Sarah A.L Merriam.
* Evento verificado por: Militza Casiano Beltrán, y Hon. Sarah A.L. Merriam
* Número de evidencia: E-1-2014-10-04 asignado al caso # C-1-2014-10-04.
* Fecha de comienzo: 6 de octubre de 2014 – 9:45 AM.
* Fecha de terminación: 6 de octubre de 2014 – 10:40 AM.
* Lugar de origen: Laboratorio Forense MCB Forensics.
* Lugar de destino: Oficina de la jueza del distrito encargado del caso.

Quinto evento:

* Descripción del evento: Devolución de la evidencia original del caso entregada por fiscalía a MCB Forensics al investigador de MCB Forensics.
* Evento verificado por: Militza Casiano Beltran y Hon. Sara A.L Merriam.
* Número de evidencia: E-1-2014-10-04 asignado al caso # C-1-2014-10-04.
* Fecha de comienzo: 6 de octubre de 2014 – 10:40 AM.
* Fecha de terminación: 6 de octubre de 2014 – 11:50 AM.
* Lugar de origen: Laboratorio Forense MCB Forensics.
* Lugar de destino: Oficina de la jueza del distrito encargado del caso.

**PROCEDIMIENTO**

El proceso de investigación puede variar según la modalidad del delito contenido. A continuación, se describe los procesos y procedimientos para recuperar, analizar y preservar la evidencia.

Se realizó u proceso en la cual se garantiza la integridad del disco duro, se procede a realizar una imagine forense hacia dos discos duros adicionales para proteger el disco dura entregado por la jueza. El proceso certifica que si ocurre algún evento que pueda afectar de modo adverso la investigación forense digital, no se vea afectado los materiales originales entregados y poder mantener como admisible cualquier información encontrada relevante al caso.

La siguiente imagen muestra el caso creado para poder hacer todo el análisis del disco duro entregado:



Figura 5: Caso creado en OSForensic

La figura 6 muestra la evidencia del archivo de texto que había indicado el acusado donde guardaba las contraseñas y nombres de usuarios que se había robado. El nombre del archivo es nicefacy0929.txt.

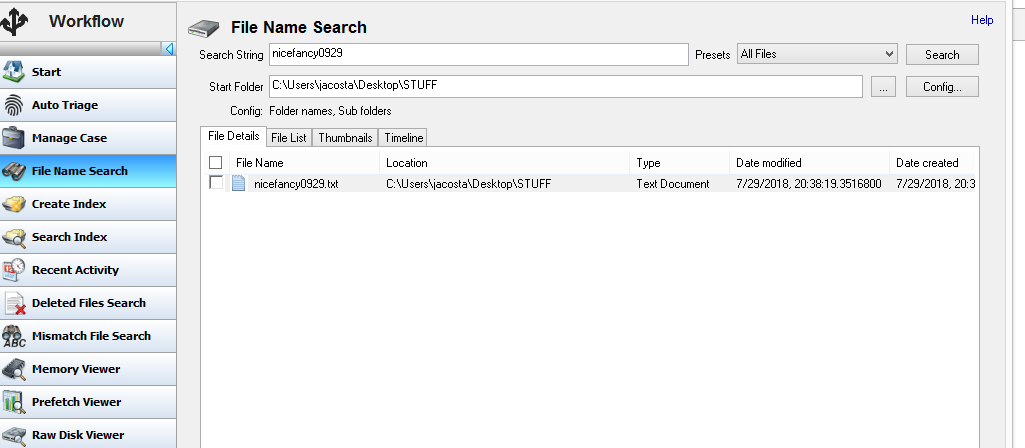


Figura 6: Evidencia del texto encontrada en el disco duro

La figura 7 muestra el contenido del archivo nicefancy0929.txt. Ahí se puede ver varios usuarios y contraseñas de los cuales se robó el acusado.

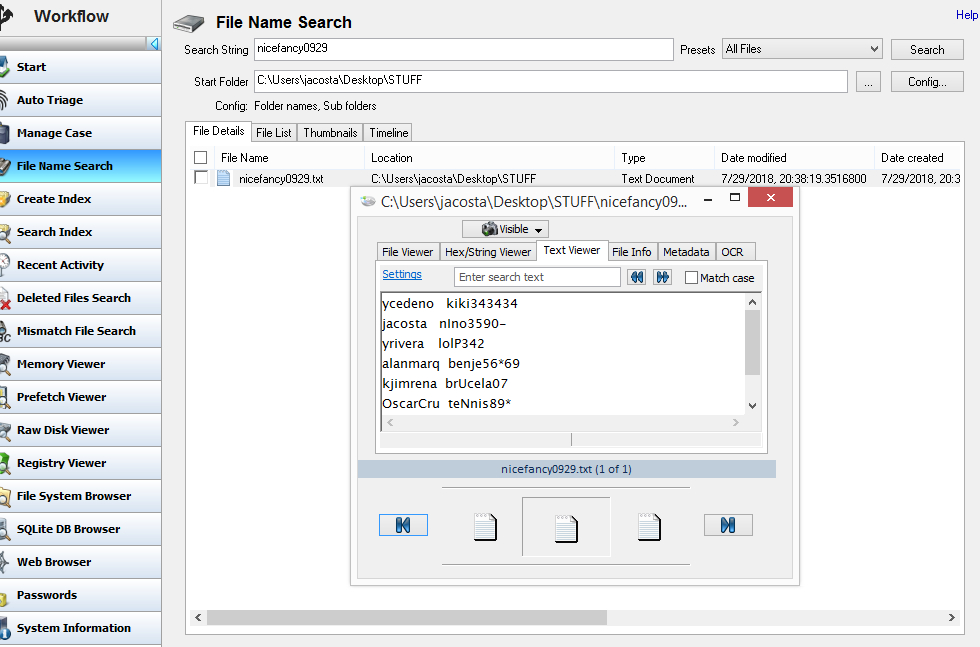


Figura 7: El contexto del nicefancy0929.txt

En la figura 8 muestra el archivo que se encontró en el disco duro, donde se puede ver una conversación que tuvo el acusado en uno de los foros. Donde indica todo lo que hace para ganarse dinero, además revela el conocimiento que tiene como hacker.

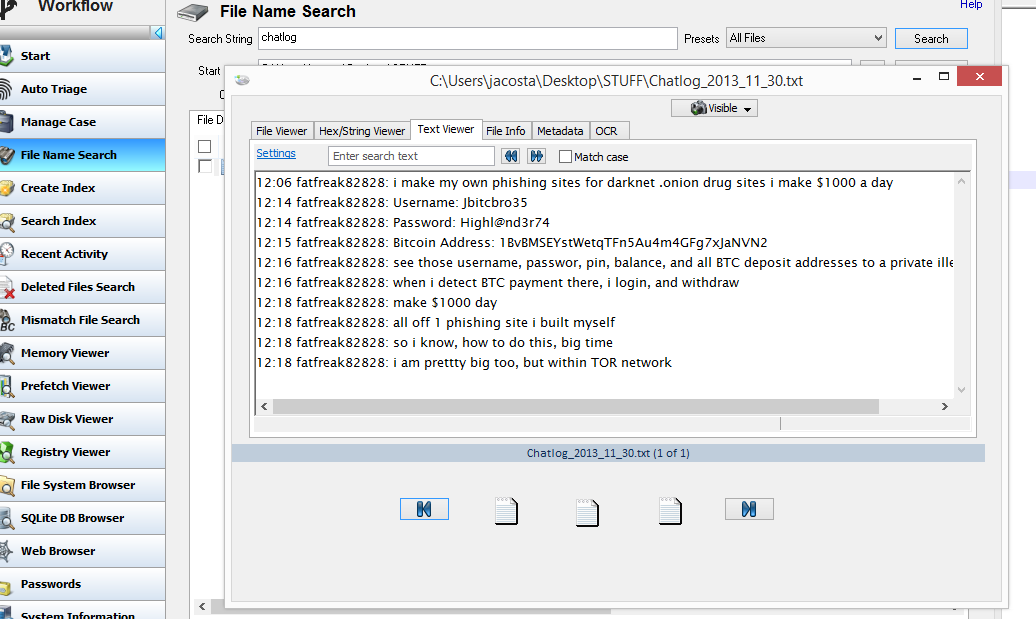


Figura 8: Evidencia de la conversación

**Conclusión**

Concluyo el reporte, el dispositivo investigado (disco duro externo) nunca fue alterado por nadie al momento de la entrega, así lo deja claro y establecido la cadena de custodia. La cadena de custodia establece que MCB Forensics recogió el equipo electrónico del cuarto de evidencia en las oficinas del FBI en presencia de la jueza a cargo del caso. El dispositivo fue entregado devuelto a las oficinas del FBI por la investigadora de MCB Forensics en presencia de la jueza a cargo del caso.

El equipo utilizado por MCB Forensics para el análisis de dicha evidencia cumple con todos los requisitos, requerimientos mínimos y estándares de la industria forense, así lo certificó MCB Forensics.

Luego del análisis realizado se pudo evidenciar que el Sr. Michael Richo sí cometió el fraude donde le robó *bitcoins* a los usuarios del mercado negro.

**SECCIÓN 5: DISCUSION DEL CASO**

Según lo que se desprende del pliego acusatorio y documentos analizados del caso USA vs. Michael Richo, el acusado se le acusa de haber robado *bitcoins* a miles de usuarios del mercado negro utilizando *phishing.* Además, se le acusa de haber cometido fraude en trasferencia electrónicas, lavado de dinero, fraude en la computadora.

Luego de un análisis riguroso de toda la evidencia encontrada dentro del disco duro tales como conversaciones, archivos de texto, se puede deducir lo siguiente:

1. Se puede confirmar que el acusado tenía en su máquina miles de contraseñas y nombre de usuarios.
2. Se puede confirmar las conversaciones que mantuvo en los foros del mercado negro donde el acusado, utilizando un nombre de usuario falsificado, admite que roba y explica como hace el fraude.

**SECCIÓN 6: AUDITORÍA Y PREVENCIÓN**

A continuación, discutiré las fallas que se encontraron donde permitieron al acusado cometer el fraude. La banca tiene que cumplir con controles de Riegos y Compliance, que es la unidad organizativa responsable de controlar la exposición del Banco. Controla el progreso del cuadro normativo y reglamentario que regula la actividad del sector bancario, financiero y asegurado garantizando el cumplimiento de la normativa actual.

La banca debe tener las siguientes gestiones de los riesgos:

* Políticas que regulan la gestión de los riesgos y en las que se incluyen limites explícitos, procedimientos y controles que determinan los procesos para la identificación, medición, control, mitigación y comunicación de los riesgos de manera eficaz.
* Herramientas que permiten identificar y medir debidamente los riesgos. Si bien estas herramientas de medición y control de los riesgos no son aprobadas expresamente por la alta gerencia.
* Herramientas de medición prospectivas (escenarios) que son realizados por algunas unidades operativas para aquellos riesgos de singular relevancia.
* Un sistema de informes de gestión, tanto de las unidades operativas como de las funciones de control de riesgos, comunicación de la exposición de los riesgos. Los informes son distribuidos entre unidades operativas y llegan hasta la alta gerencia.

**Hallazgos Detallados**

Como parte de la auditoría realizada al Bank of America se encuentra los siguientes hallazgos relevantes.

1. El mecanismo para validar las trasferencias electrónicas falló:
   * Condición: no se aplicó o no existe un mecanismo que valide el origen de las transferencias electrónicas.
   * Criterio: se entiende que, de ser aplicado dicho control, se puede detectar a tiempo un fraude.
   * Causa: esta condición se debe a la falta de controles para la validación de las transferencias electrónicas.
   * Efecto: El impacto en este caso es la perdida monetaria y la continuidad del fraude.

Se recomienda implantar los siguiente:

* Establecer controles más rigurosos en el cual validen la procedencia de las transferencias electrónicas.
* Realizar un reporte que corra a diario de las transferencias electrónicas que no cumplan con las condiciones establecidas. Tener un personal que valide ese reporte.

**SECCIÓN 7: CONCLUSION**

La oportunidad para cometer fraude la tenemos todos, sólo los que les gusta el riesgo lo terminan cometiendo. Como pudieron observar en la sección 4, existen herramientas que nos pueden ayudar a esclarecer los casos de fraude. Herramientas que son sencillas de usar sólo tiene que poseer conocimiento utilizando varios programas de computadora.

En este caso se pudo observar que el acusado, Michael Richo, vio la oportunidad y ya que tenía el conocimiento de hacker desde que era niño. Además, que vio que podía hacer dinero fácil con tan solo engañar a varios usuarios en el mercado negro. Se pudo observar en este caso las fallas de los controles esenciales para detectar un fraude en proceso.

Para concluir. Se pudo observar como este individuo comete el fraude y se burla de las personas. El acusado no le importó el daño que le ocasionó a las personas. Aprovechó su conocimiento que pudo utilizarlo para un bien ya que cualquier empresa podía contratarlo, pero decidió irse por el lado fácil e ilegal terminando en la cárcel.

**SECCIÓN 8: REFERENCIA**

Banco Medioladum (2018). Recuperado de:

<https://www.bancomediolanum.es/es-ES/gobierno-corporativo-y-remuneraciones/mecanismos-de-control.html>

Horwitz, A. (2018, 2 enero). What is Bitcoin? A Simple (but through explanation).

Recuperado de <https://99bitcoins.com/bitcoin-whiteboard-tuesday-what-is-bitcoin/?gclid=Cj0KCQiA2snUBRDfARIsAIGfpqFqY75QkBeL1Vn14lpWJcHtu_aotWzNQNxpnGLj4LzbbOssdz0I5DkaAjRlEALw_wcB>

Madeira, A. (2018, 29 mazo) 7 ways criminals steal your bitcoins Recuperado de:

<https://bitcoinist.com/7-ways-criminals-steal-your-bitcoins/>

Michael Richo Criminal Complaint. (2016, 4 octubre).

Recuperado de <https://www.scribd.com/document/327102542/Michael-Richo-Criminal-Complaint>

Tecnósfera (2018, 31 mayo). Cibercriminales optan por suplantar páginas de redes sociales.

Recuperado de: <http://www.eltiempo.com/tecnosfera/novedades-tecnologia/casos-de-phishing-en-redes-sociales-en-2018-224936>

United States of America v. Michael Richo (2016). Recuperado por: [www.pacer.gov](http://www.pacer.gov)

United States of America v. Olajide Abraham Eyitayo (2018). Recuperado de:

[www.morelaw.com](http://www.morelaw.com)

United States of America v. Konrads Voits (2017). Recuperado de: [www.morelaw.com](http://www.morelaw.com)

## United States of America v. Karim Baratov, a/k/a “Kay,” a/k/a/Karim Taloverov, a/k/a Karim

## Akehmet Tokbergenov (2017). Recuperado de: [www.morelaw.com](http://www.morelaw.com)

# Vadeolmillos, C. (2018, 25 julio) El phishing, entre las principales amenazas para el correo

# electrónico de las empresas. Recuperado de:

# <https://www.muycomputerpro.com/2018/07/25/phishing-amenazas-correo-electronico->empresas

Wikipedia The Free Encyclopedia(s.f) Bot. Recuperado de: <https://en.wikipedia.org/wiki/Internet_bot>

Wikipedia The Free Encyclopedia(s.f). Bitcoin

Recuperado de: <https://en.wikipedia.org/wiki/Bitcoin>

Wikipedia The Free Encyclopedia (s.f.) Bitcoin Fog.

Recuperado de: <https://en.wikipedia.org/wiki/Bitcoin_Fog>

Wikipedia The Free Encyclopedia (s.f). Cryptocurrency Tumbler. Recuperado de:

<https://en.wikipedia.org/wiki/Cryptocurrency_tumbler>

Wikipedia The Free Encyclopedia (s.f). Local Bitcoins.

Recuperado de: <https://en.wikipedia.org/wiki/LocalBitcoins>

Wikipedia The Free Encyclopedia (s.f). Blockchain.

Recuperado de: <https://en.wikipedia.org/wiki/Blockchain>

Wikipedia The Free Encyclopedia (s.f). Phishing.

Recuperado de: <https://en.wikipedia.org/wiki/Phishing>

Wikipedia The Free Encyclopedia (s.f). Computer Security. Recuperado de:

<https://en.wikipedia.org/wiki/Exploit_(computer_security)>

Wikipedia The Free Encyclopedia (s.f). Rooting Recuperado de:

<https://en.wikipedia.org/wiki/Rooting_(Android)>

Wikipedia The Free Encyclopedia (s.f). Backdoor Recuperado de:

<https://en.wikipedia.org/wiki/Backdoor_(computing)>

Wikipedia The Free Encyclopedia (s.f). Internet Bot.

Recuperado de: <https://en.wikipedia.org/wiki/Internet_bot>

Wikipedia The Free Encyclopedia (s.f). Botnet.

Recuperado de: https://en.wikipedia.org/wiki/Botnet