EDP UNIVERSITY OF PUERTO RICO INC.

RECINTO DE HATO REY

ESCUELA GRADUADA

PROGRAMA DE MAESTRIA EN SISTEMAS DE INFORMACION

ESPECIALIDAD EN SEGURIDAD DE INFORMACION E INVESTIGACION DE FRAUDE

FRAUDE DE IDENTIDAD AGRAVADO, SUBASTAS FALSAS Y FRAUDE DE CRIPTOMONEDA

ANÁLISIS DEL CASO: UNITED STATE OF AMERICA VS. BOGDAN NICOLESCU, TIBERIU DANET Y RADU MICLAUS

NUMERO DE CASO: 1:16-cr0024

PREPARADO POR

JOSE RAMOS SOTO

Marzo,2019

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

FRAUDE DE IDENTIDAD AGRAVADO, SUBASTAS FALSAS Y FRAUDE DE CRIPTOMONEDA

ANÁLISIS DEL CASO: UNITED STATE OF AMERICA VS. BOGDAN NICOLESCU, TIBERIU DANET Y RADU MICLAUS

Numero de caso: 1:16-cr0024

Preparado por:

Jose Ramos Soto

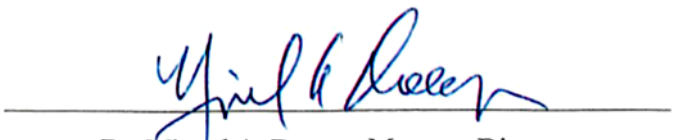
Ha sido aceptado como requisito parcial para el grado de:

Maestría en Sistemas de Información:

Especialidad en Seguridad de Información e Investigación de Fraude

Marzo,2019

Aprobado por:



Dr. Miguel A. Drouyn Marrero, Director

Agradecimientos

Quiero dar gracias a Dios por brindarme la oportunidad y la capacidad de poder cumplir una vez más mi sueño. Desde que di mis primeros pasos él cuida de mí. Mi familia quienes son los que me llenan de consejos de motivación para nunca rendirme. Mi papa que cada día que pasa me brinda su inmenso apoyo y ora por mí para que siempre alcance cada uno de mis sueños anhelados. Ambos nos identificamos porque somos luchadores, humildes, trabajadores, pero lo más importante es que tenemos nuestros valores por delante. Todos nuestros pasos los presentamos frente a Dios, siendo él nuestro guía oficial. Agradecido con Nashalie Pérez, Angela Pérez, Brendaliz Ortiz, Edwin Valentín y Edwin Jose que han estado mano a mano conmigo durante todo este transcurso académico. Muy agradecido con cada uno de ustedes.

Gracias a la facultad de profesores del EDP University por depositar su conocimiento y experiencia en mi carrera profesional. Agradecido porque pude adquirir las herramientas que serán de utilidad para crear y organizar mi futuro, obteniendo así cada uno de mis sueños anhelados. Nunca dudes de tus capacidades porque todos nuestros sueños se pueden hacer realidad, pero hay que luchar por ellos. Bendiciones a todos.

Tabla de Contenido

Tabla de Figuras

SECCIÓN I: INTRODUCCIÓN Y TRASFONDO

Introducción:

En el período actual el uso de la internet ha estado accesible a gran mayoría en distintos países. Por consiguiente, la misma puede ser manejada de manera positiva como negativa. Un alto volumen en la sociedad es el resultado para que los usuarios en las redes cibernéticas aumenten. Se ha observado que los jóvenes de 25 años o menos son los líderes en utilizar las redes de navegación y mayormente las paginas sociales como Facebook, Instagram, EBay, Amazon, etc. Además, no solamente eso, varias compañías como lo son los bancos cuentan con aplicaciones que los usuarios pueden acceder a través de su teléfono móvil, computadoras y tabletas para un mayor manejo de sus transacciones. El conocimiento en ellos respecto a las amenazas que se pueden enfrentar cuando integra a la web es escaso. El análisis de la investigación se basa en la teoría del triángulo de fraude desarrollado por Donald R. Cressey (Wells, 2013).

En los últimos años las amenazas en la internet van aumentando a un nivel drástico ya que a través de ellas se pueden ocasionar fraudes, perdidas de alta cantidad de dinero a empresas y usuarios activos. La mayoría de las veces son realizadas por los hackers. Ellos se encargan de ver fallas en cualquier puerto en la red para atacar y adquirir lo que ellos necesitan de las víctimas. El correo electrónico fue uno de los progresos que aportó el internet, ya que facilitó enormemente la comunicación entre las personas y significó un aumento de productividad en el ámbito de las empresas. Al integrarse, los costos de comunicaciones comenzaron a disminuir.

El riesgo de fraude y su materialización en las organizaciones es una preocupación importante para quienes lideran e integran por cuanto este mal se esté generalizando. Esto afecta la consecución de los objetivos, ocasiona impactos negativos financieros y afecta la imagen tanto de las empresas privadas como las entidades de gobierno, al igual que incrementa el inexorable

avance de la corrupción. La educación y el desarrollo de medidas legales son sumamente importante para el control del crimen. Esto abarca una serie de grupos que si se toma acción se puede minimizar los fraudes. Los grupos son:

- El gobierno que es el encargado de dirigir e integrar las leyes de nuestro país.
- La sociedad civil.
- Los proveedores de internet.
- Las instituciones educativas en nuestro país, ya que es donde se comienza a definir los jóvenes profesionales del futuro donde pondrán en práctica la ética y los valores adquiridos.

Descripción del caso:

Caso: United State of America Vs. Bogdan Nicolescu, Tiberiu Danet, y Radu Miclaus

No. de caso: 1:16-cr0024

Partes en el caso:

Acusados:

Véase la figura 1: Fotos de acusados
(Fuente de foto: American Security, 2016. https://americansecuritytoday.com/3-extradited-face-us-charges-4m-cyber-fraud-scheme-video/romanians/.)

1. Bogdan Nicolescu, Bucarestino, Rumania.
2. Tiberiu Danet, Bucarestino, Rumania.
3. Radu Miclaus, Bucarestino, Rumania.
4. Bayrob Group, Grupo de hacker pertenecientes de Bucarest, Romania.

Entidades relacionadas con el caso (victimas):

1. Western Unión.
2. Symantec Corporations.
3. Norton Antivirus.
4. Servicios de Impuestos Internos de los Estados Unidos (IRS).
5. Usuarios de Facebook.
6. Usuarios de PayPal.
7. Usuarios de Gmail.
8. Usuarios de Walmart.
9. Usuarios de Yahoo!

Abogados:

1. Duncan T. Brown, Asistente de Abogado en los Estados Unidos en el estado de Ohio.
2. Om Kakani. Asistente de Abogados en los Estados Unidos en el estado de Ohio.
3. Brian Levine, Asistente de Abogados en los Estados Unidos en el estado de New Jersey.

Fiscales:

1. Carole S. Rendon, Ex Fiscal de los Estados Unidos para el Distrito Norte de Ohio.
2. Leslie R. Caldwell, Procuradora General Adjunta de la División Penal del Departamento de Justicia de los Estados Unidos

Agente encargado:

1. Stephen D. Anthony, Agente a cargo de la División de Cleveland.

Juez:

1. Gran Jurado, Gaughan, Corte Federal de Distrito de Ohio.

Trasfondo

Este trabajo investigativo está enfocado en el área del crimen cibernético donde se presentará 3 esquemas de fraudes ocasionados por 3 individuos pertenecientes de Rumania. El caso de USA vs Bogdan Nicolescu, Radu Miclaus y Tiberius Danes (2016), ha transcurrido a ser uno de los esquemas de fraudes más técnico de la web. Los acusados en este caso están compuestos en por Bogdan Nicolescu, 34, Tiberiu Danet,31, y Radu Miclaus 34, pertenecientes al grupo Bayrob. Desde el 2007, son el grupo de hackers que se encargaron de realizar ataques a más de 60,000 a 160,000 computadoras, la mayor parte en los Estados Unidos. Crearon un malware llamado el Troyano de Bayrob que fue el protagonista para realizar mencionada felonía. Ocasionaron fraudes bancarios en el cual robaron una gran cantidad de dinero. Engañaron a las víctimas con paginas falsas, correos electrónicos fraudulentos, subastas falsas, robo de números de tarjetas de créditos, etc. Organizaron una gama de esquemas de fraude donde su primer

esquema ocasionado fue el de robo de identidad, el segundo fue el esquema en subasta y por último el esquema de criptomoneda.

La investigación o actividad ilegal, se detectó en el 2007 cuando una mujer informó que pagó $ 8,000 por un vehículo que nunca recibió y creía que su computadora estaba infectada en cual el caso fue investigado por el FBI con asistencia de la Policía Nacional de Rumania (Jen Steer, 2016). La compañía de Symantec le notificó al FBI, llamó a las autoridades rumanas, que a su vez arrestaron a las pandillas a principios del 2016. La acusación fue presentada por la Oficina del Fiscal de los Estados Unidos en el Distrito Norte de Ohio. Los abogados adjuntos de los Estados Unidos, Duncan T. Brown y Om Kakani, están procesando el caso junto con Brian Levine, abogado principal de la Sección de Delitos Informáticos y Propiedad Intelectual del Departamento de Justicia. El FBI dirigió la investigación de la operación de Bayrob, con la asistencia de la Policía Nacional de Rumania.

Descripción de los hechos:

Según los documentos del caso USA vs Bogdan Nicolescu, Tiberiu Danet y Radu Miclaus (2016), la Fiscal Federal Carole S. Rendon y el FBI lo cual estos tres individuos fueron acusados de operar una conspiración de fraude cibernético en la que infectaron 60,000 computadoras, enviaron correos electrónicos maliciosos y robaron al menos $4 millones de dólares. El agente a cargo fue Stephen D. Anthony. Además, fueron detenido en su tierra natal de Rumania. Según la acusación presentada en el Tribunal de Distrito de EE. UU. en el Norte de Ohio, operaron colectivamente en una conspiración criminal desde Bucarest Rumania. Cada uno de ellos está acusado de conspiración por cometer fraude electrónico, conspiración para traficar con marcas de servicio falsificadas, robo de identidad agravado, conspiración para cometer lavado de dinero y 12 cargos de fraude bancario. Muchas de las víctimas, que perdieron entre $

8,000 y $ 16,000 cada una, son del noreste de Ohio. Comenzaron en el 2007 con el desarrollo del malware propietario, que se difundió a través de correos maliciosos que pretendían ser legítimos de entidades como *Western Union*, *Norton Antivirus* y el *IRS*. Cuando los destinatarios hacían clic en un archivo adjunto, el malware se instalaba silenciosamente en su computadora. Recolectaba las direcciones de correos electrónicos de las computadoras infectadas, como las listas de contactos.

Las versiones del troyano de Bayrob fue con lo que los acusados infectaron y controlaron más de 60,000 computadoras individuales, principalmente en los Estados Unidos. El control de ellas permitió a los demandados recopilar información personal, como información de tarjetas de créditos, nombre de usuarios y contraseñas. Bloqueaban los sitios de la web asociados con la policía. Además, permitió que el grupo de demandados usara la capacidad de procesamiento de la computadora para resolver algoritmos complejos para el beneficio financiero del grupo, un proceso conocido como minería de criptomoneda. Utilizaron credenciales de correo electrónico robadas para copiar los contactos de las víctimas. También activaron archivos que obligaron a las computadoras infectadas a registrar cuentas de correo electrónico con *AOL* que es un servicio de web mail.

Cuando las víctimas con computadoras infectadas visitaban sitios web como *Facebook*, *PayPal*, *eBay* u otros, los demandados interceptaban la solicitud y redirigían la computadora a un sitio web casi idéntico que habían creado obteniendo así las credenciales de la cuenta. Utilizaron la información de tarjetas de crédito robadas para financiar su infraestructura criminal, incluyendo el alquiler de espacio en el servidor, el registro de nombres de dominio con identidades ficticias y el pago de redes virtuales privadas (*VPN*), que ocultaban aún más sus identidades. Utilizaron una doble capa de proxis, uno en Rumania y otro en los Estados Unidos.

Symantec permaneció escondido, observando estos servidores proxy durante un año y medio hasta que uno de ellos filtro información que permitió a los investigadores rastrear a cada sospechoso. Para el 2011 dice que comenzó a crear una imagen de la infraestructura de back-end de Bayrob. Usaron correos cifrados con *PGP* y mensajes instantáneos *XMPP OTR* (*Off-The-Record*) para coordinar negocios sin ser interceptados.

Colocaron más de 1,000 listados fraudulentos de automóviles, motocicletas y otros bienes de alto precio en *eBay* y sitios de subastas similares. Las fotos de los artículos estaban infectadas con malware, que redirigía las computadoras que hacían clic en la imagen a páginas web ficticias diseñadas por los demandados para parecerse a las páginas legítimas de *eBay* y adyacentes. Los usuarios pagaban la mercancía a los agentes de custodia fraudulentos, quienes a su vez transfirieron el dinero a otros en el Este de Europa, que a su vez se lo dieron a los acusados. Las victimas nunca recibieron la mercancía y tampoco el dinero. Esto ocasionó una pérdida de 4 millones de dólares. Para el 2014, la pandilla comenzó a modificar su malware para recopilar números de tarjetas de crédito y otra información de computadoras afectadas, detalles que usaron para realizar compras fraudulentas por su cuenta, sin tener que engañar a las víctimas para que inicien la transferencia. Un observador remoto habría descubierto que algo estaba mal solo al ver la red de computadoras infectadas con Bayrob, que creció de unas 1,000 computadoras en 2007 a unos 50,000 bots en 2014, y hasta 300,000 este año. (Frolik 2017).

El grupo Bayrob lavó este dinero mediante la contratación de "agentes de transferencia de dinero" y creó compañías ficticias con sitios web fraudulentos diseñados para dar la impresión de que eran negocios reales comprometidos en transacciones financieras legítimas. El dinero robado a las víctimas se transfirió a estas compañías fraudulentas y luego a su vez a las oficinas de *Western Union* o *Money Gram* en Rumania. Las “mulas monetarias” europeas utilizaron

documentos de identidad falsos para recolectar el dinero y entregarlo a los acusados, de acuerdo con la acusación. Esta red de más de 60,000 computadoras se conoce como *Bayrob Botnet*. Es controlado por el grupo de Bayrob mediante uno o más comandos y servidores de control (*C&C servers*), que permite al grupo de Bayrob enviar códigos y emitir comandos para cualquier o todos los bots en mencionada red. Para garantizar la estabilidad y confiabilidad de la *Bayrob Botnet* contra la interrupción por parte de las autoridades policiales u otras interrupciones, el grupo Bayrob pagó para que sus servidores sean alojados por proveedores de servicios de Internet confiables en los Estados Unidos. Además, mantenían servidores *C&C* redundantes con los diferentes *ISP* con una copia de seguridad periódica de los datos e información en esos servidores.

Para recibir comandos del grupo Bayrob, los robots se registraron automáticamente con los dominios de Internet registrados por el grupo Bayrob a través de computadoras infectadas, utilizando la identidad robada y la información de la tarjeta de crédito. Estos dominios fueron generados automáticamente por el algoritmo de generación de dominios del trojano de Bayrob y tenían nombres sin sentido como *storeladder.net, lookuncle.net o neededfahter.net.* Para ocultar sus identidades los miembros del grupo no se conectaban directamente con el servidor de *C&C*, sino se conectaban utilizando varios proxys. La comunicación entre los miembros del grupo Bayrob y la infraestructura utilizo un *shell* seguro, que es un protocolo de red cifrado para permitir que el inicio de sesión remoto y otros servicios de red operen de manera segura en una red no segura.

Cuando se comunican entre sí, utilizan un cifrado seguro de ambos extremos. Cifraron los datos adjuntos y utilizaron otros métodos más seguros de comunicación, incluida una tecnología de mensajería instantánea conocida como *Jabber*. Esta tecnología era administrada

por el grupo Bayrob mediante un servidor privado y seguro. Las computadoras infectadas recibieron órdenes de enviar correos electrónicos maliciosos o mensajes instantáneos a una lista de cuentas de destino. Utilizaron la potencia del procesamiento de las computadoras para resolver algoritmos complejos para el beneficio financiero del grupo. Deshabilitaron la protección contra malware de la víctima bloqueando el acceso de la víctima a sitios web asociados con la policía. Inyectaron paginas falsas en sitios web legítimos, como eBay, para hacerle creer a las víctimas que están recibiendo y siguiendo las instrucciones de los sitios web correctos, que se activan siguiendo las direcciones del grupo Bayrob. Los servidores del *C&C* están ubicados en los Estados Unidos.

Sus arrestos fueron resultados de una investigación policial, asistida por Symantec, que duro al menos 8 años.

Acusaciones, Cargos y Penalidades:

Desde el 2007 hasta la fecha de la acusación en el Distrito Norte de Ohio por parte de los acusados Bogdan Nicolescu, Tiberiu Danet y Radu Miclaus cometieron los siguientes delitos contra los Estados Unidos:

Cargo 1: 18 USC 1343 y 1349: Fraude por cable, radio o televisión.

En marzo 7 de 2014 el servidor *C&C* comenzó a instalar un archivo titulado "*casper.js"* en las computadoras infectadas. El archivo mencionado contenía el código utilizado por el equipo de Bayrob para realizar el esquema de infección al indicar a los sistemas infectados registrar los dominios de *Yahoo!* automáticamente, robar correos electrónicos en la web y con el interés de seguir con el grupo.

Cargo 2-13: 18 USC 1343: Acusación por Fraude por cable

En o alrededor de las siguientes fechas, las víctimas transfirieron fondos a mulas de dinero con base en los EE. UU. que trabajaban para el Grupo Bayrob a través de una transferencia bancaria bajo la creencia errónea de que estaban comprando un artículo real que figura en el sitio auténtico de eBay. En la realidad, cada transacción involucró a artículo no existente que figura en una página fraudulenta de *eBay*, creado por Bayrob Group, que fue inyectado en la computadora de la **v**íctima por el troyano Bayrob, cada uno de los cuales era una comunicación por cable interestatal o extranjera que constituía una ofensa separada y distinta.

Cargo 14: 18 U.S.C. §371: Acusación por Conspiración:

Entre 2014 y 2015, los miembros del Grupo Bayrob, a través del acceso no autorizado a las computadoras crearon el troyano Bayrob, instalaron un archivo adicional titulado "*miner_forced*" en al menos 33,000 computadoras, incluidas las computadoras infectadas a continuación, para forzar a las computadoras a usar su poder de computadora para explotar la crueldad, lo que daña a las computadoras infectadas al reducir significativamente el poder de procesamiento disponible para el usuario, y cada uno de ellos constituye un acto separado para promover la conspiración.

Cargo 15: 18 U.SC. § 2320(a)(1)): Acusación por Conspiración para Traficar en Marcas de Servicio Falsificadas

El grupo Bayrob envía marcas falsas y marcas de servicio asociadas con eBay, Facebook, Gmail y otros a al menos 40,000 víctimas, incluidas las víctimas que se enumeran a continuación, en un esfuerzo por engañar a estas víctimas para que les envíen su información de tarjeta de crédito personal, información de cuenta, o instalar malware en sus computadoras.

Cargo 16- 20: 18 U.S.C. §§ 1028A(a)(1) y (2): Acusación por Robo de Identidad Agravado

El grupo Bayrob recolectó y usó más de 500 tarjetas de crédito robadas a través de su esquema, incluidas las tarjetas de crédito propiedad de las víctimas.

Los miembros del Grupo Bayrob sabían, y tenían motivos para saberlo, que la información recopilada era de individuos reales porque los medios por los cuales se recopiló fueron diseñados específicamente para la respuesta requerida y la acción afirmativa de la víctima para proporcionar su propia información de verificación. Además, la información de la tarjeta de crédito era de individuos reales porque los miembros utilizaron con éxito las tarjetas para realizar compras y a menudo, repetían las compras durante un período prolongado.

Cargo 21: 18 U.SC. § 1956(h): Acusación por Conspiración para cometer lavado de dinero

El Grupo Bayrob pudo transferir más de 1,100,000 al exterior a través de *Western Union*. Los ingresos de los cables recibidos por el Grupo Bayrob estaban destinados a dividirse de la siguiente manera; Nicolescu recibió el 25%, Danet recibió el 25% y Miclaus recibió el 10%. Los fondos restantes se dividirían entre personas desconocidas para el Gran Jurado.

Definición de términos

Botnet – es un conjunto de bots que funcionan de forma autónoma y automática. El que desarrolla esta red puede controlar todos los ordenadores y servidores que hayan sido afectados (Arimetrica Digital).

Bot – los bot son programas que exploran la web. Tienen diferentes propósitos, como indexar páginas web a motores de búsqueda o cosechar direcciones de correos electrónicos para los spammers (Arimetrica Digital).

Criptomoneda - son monedas virtuales que pueden ser intercambiadas y operadas como cualquier otra divisa tradicional, pero están fuera del control de los gobiernos e instituciones financieras. (IG Group, 2003).

Criptominio - es la técnica de usar el poder de procesamiento de una computadora para resolver las matemáticas detrás de la generación de criptomoneda o la validación de la transacción de criptomoneda. (Oracle, 2014)

Dirección de protocolo de Internet (IP address) - se define como una etiqueta numérica asignada a un dispositivo conectado a Internet que proporciona información que es útil para identificar y localizar el dispositivo. (Oracle, 2014)

ISP – es un proveedor de servicio de internet. Es decir, es la empresa que le vender internet a los usuarios. (Oracle, 2014)

Malware: es un software malicioso o intrusivo que se instala en una computadora sin el conocimiento o permiso del propietario. (Oracle, 2014)

Mensajería instantánea (jabber) -puedes enviar mensajes a usuarios desconectados, conectar a tu cuenta desde varios sitios al mismo tiempo, conectar a otras redes como MSN, AIM o Yahoo!. (Oracle, 2014)

Nombre de dominio - se utiliza para identificar la dirección IP de un sitio web en Internet. (Oracle, 2014)

Proveedor de servicios de Internet (ISP) - en una organización que brinda servicios para acceder, usar o participar en Internet. El servicio que suelen proporcionar los ISP incluye acceso a Internet,

tránsito de Internet, registro de nombres de dominio, servicios de correo electrónico y alojamiento web. (Oracle, 2014)

Proxy – es un servidor que actúa de forma intermediaria entre una computadora y la internet. (Oracle, 2014)

Red privada virtual (VPN) - es una tecnología que crea una conexión de red segura a través de una red pública, como Internet o una red privada que es propiedad de un proveedor de servicios de Internet. Al usar VPN, un usuario puede ocultar su verdadera dirección IP de aquellos con quienes se está comunicando. (Oracle, 2014)

SECCION II. REVISION DE LITERATURA

Introducción:

El fraude se considera como una de las industrias criminales más grandes en la sociedad, aumentando en épocas donde la gente necesita dinero tales como la Navidad, Fin de Año, etc. Las victimas afectadas son las que tienen un conocimiento deficiente sobre las amenazas que se alojan en la Internet. Además, el fraude en servicios en líneas, como lo son los correos electrónicos que son los más utilizado entre usuarios en aplicaciones, industrias como PayPal que mantienen sus procesos de transacciones de pagos y cuentas de bancos protegidas en la web, paginas sociales como Facebook, Instagram, Twitter, etc. cada día las perdidas por ataques fraudulentos van en aumento. El fraude en la actualidad continúa siendo un riesgo preocupante a nivel mundial, ninguna empresa o industria parece estar a salvo de este riesgo sin importar el tamaño o sin han dedicado recursos para combatir el fraude. La imagen para cada industria es sumamente importante. El análisis de la investigación se basa en la teoría del triángulo de fraude desarrollado por Donald R. Cressey (Wells, 2013).

A veces la mayor parte del fraude lo tenemos tan de cerca que no se dan cuenta. De este modo cualquier fallo que se enfrente, ya sea en los controles u otros métodos dentro de la empresa, va a dar sospecha de que el fraude los podrá tocar de cerca. Existen controles que se deben aplicar en nuestro diario vivir, ya sea utilizando antivirus altamente potentes, guardianes de páginas web para no tener acceso a paginas no confiables y se bloqueen automáticamente, un firewall que sea seguro, limitar los accesos cuando se asignan puestos, verificar a diario informes importantes, no exponer información confidencial para así proteger a los usuarios, clientes, empleados dentro de una empresa o industria en particular. Y no solamente eso, también cuidar su ética y postura, ante todo.

Un fraude puede generar grandes pérdidas a una empresa y más grave aún dañar su reputación. El propósito de esto es de que debemos de tomar las debidas precauciones al visitar la web mayormente, cuando se va a hacer de uso propio. Informarte a diario sobre los nuevos riesgos que pueden salir a la luz para que obvies las amenazas siguientes que te pueden afectar peligrosamente. Las medidas jurídicas tienen un rol clave en la prevención y la lucha contra el delito cibernético. Se requieren a gran medida de este tipo en todas las áreas, incluyendo la tipificación, los poderes procésales, jurisdicción, la cooperación internacional y la responsabilidad de los proveedores de servicio de Internet, A nivel nacional, tanto las leyes existentes como las nuevas sobre delito cibernético, suelen estar relacionadas con la criminalización, lo cual indica un interés predominante en establecer figuras delictivas específicas para los principales actos de delito cibernético.

Fraudes Involucrados

Robo de identidad

El robo de identidad se produce cuando una persona adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la intención de efectuar o vincularlo con algún fraude u otro delito (Labaca Castro, 2011).

Lavado de dinero:

El lavado de dinero es el proceso a través del cual es encubierto el origen de los fondos generados mediante el ejercicio de algunas actividades ilegales. (Comisión Nacional Bancaria y de Valores, 2010).

Apropiación ilegal:

La apropiación ilegal es toda persona que ilegalmente se apropiare sin violencia ni intimidación de bienes muebles, pertenecientes a otra persona (LexJuris).

Fraude:

El fraude es acción que revela en su autor la voluntad de perjudicar a otro, o de violar ciertas prescripciones legales. (Enciclopedia Jurídica, 2014).

Estadísticas:

Yong, (2018) indica que en diciembre pasado los ataques de malware para robar datos financieros se incrementaron a un 22.4%, en tanto que la compañía de seguridad RSA calcula en US$9.100 millones al año de pérdidas por phishing y un estudio por el FBI estima en US$2.300 millones del daño causado en el mundo en los últimos tres años solo por *ramsonware*, uno de los delitos informáticos de moda de estos días.

En un 52% de casos, el delito es de origen interno y el 24% de las veces, es cometido por alguien a la Alta Gerencia. Actualmente un 53% de compañías latinoamericanas indican haber sido víctimas de fraude en los últimos 2 años; evidenciando un crecimiento significativo, ya que en el 2016 solo un 28% manifestó haberlo experimentado. *Kapersky Lab* detecto cerca de 400 millones de intentos de ataques de virus en América Latina para el 2015, lo cual se traduce en más de 30 incidentes por segundos. *Brasil* encabeza 27.6 millones de intentos de infección, y es el numero 18 a escala mundial. México ocupa el segundo puesto en América Latina en ataque por infección de virus con un 15.9% de incidentes. Se adjuntan a la lista Colombia con 5.1%, Perú con 4.3%, Venezuela con 2 millones y Chile con 1.6 millones. (citado por Yong, 2018)

Labaca Castro (2011) en un estudio publicado en el Manual de la Naciones Unidas para la prevención y control de delitos informáticos, el 90% de los delitos realizados mediante

computadora fueron ejecutados por empleados de la propia empresa afectada. Así mismo otro estudio realizado en América del Norte y Europa indico el 73% de las intrusiones informáticas cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

Según Malby Steve (2013), las encuestas de victimización representan una base más sólida para la comparación. Estas muestran que la victimización individual por delito cibernético es mucho mayor que por las formas de delitos 'convencionales'. Las tasas de victimización por fraude en línea con tarjetas de crédito, robo de identidad, respuesta a intentos de suplantación (phishing) y por experimentar acceso no autorizado a una cuenta de correo varían entre el 1% y el 17% de la población con acceso a Internet de 21 países de todo el mundo, en comparación con tasas de robo, asalto y robo de coches de menos de 5 por ciento en los mismos países. Las tasas de victimización por delitos cibernéticos son más altas en los países con niveles menores de desarrollo, lo que destaca la necesidad de fortalecer los esfuerzos de prevención en esos países.

Las empresas del sector privado en Europa reportan tasas de victimización similares entre el 2% y el 16% por actos como el acceso no autorizado a los datos por intrusión o phishing. Las herramientas delictivas para estos delitos, como las redes zombis o "*botnets*", tienen un alcance mundial. En 2011 más de un millón de direcciones IP únicas a nivel mundial funcionaban como servidores de mando y control de redes zombi o *"botnet*". El contenido en Internet también representó una inquietud considerable para los gobiernos. El material al que se dirigen los esfuerzos de remoción no solo incluye la pornografía infantil y el discurso de incitación al odio, sino también contenido relacionado con la difamación y la crítica a los gobiernos, lo cual despierta en algunos casos inquietudes relacionadas con las leyes de derechos humanos. Se calcula que casi el 24 por ciento de todo el tráfico mundial de Internet viola los derechos de

autor, con las descargas de material compartido de pares a pares (P2P) particularmente numerosas en países de África, América del Sur y Asia Occidental y Austral. (citado por

Leyes Aplicables

Principales, Titulo 18 U.S. Código § 2

Este código establece que:

(a) El que cometa una ofensa contra los Estados Unidos o ayude, imite, asesore, ordene, induzca o procure su comisión, es punible como principal.

(b) Quien intencionalmente hace que se realice un acto que, si él u otro cometiera directamente sería un delito contra los Estados Unidos, es punible como principal.

Conspiración para cometer ofensas o defraudar a los Estados Unidos, Titulo 18 U.S. Código § 371

Este código establece que:

Si dos o más personas conspiran para cometer un delito contra los Estados Unidos, o para defraudar a los Estados Unidos, o cualquier agencia de estos en cualquier forma o para cualquier propósito, y una o más de esas personas hacen cualquier acto para llevar a cabo el objeto de En la conspiración, cada uno será multado bajo este título o encarcelado por no más de cinco años, o ambos. Sin embargo, si la ofensa, cuya comisión es el objeto de la conspiración, es un delito menor únicamente, el castigo por dicha conspiración no deberá exceder el castigo máximo provisto por tal delito menor.

Robo de identidad Agravado, Titulo 18 U.S. Código § 1028 (a)(1) y (2)

Este código establece que:

(1) En general:

Quien desee durante y en relación con cualquier violación de delito grave enumerada en la subsección (c), a sabiendas transfiere, posee o utiliza, sin la autoridad legal, un medio de identificación de otra persona será, además del castigo provisto para tal delito, será sentenciado a una pena de prisión de 2 años.

(2) Ofensa de terrorismo:

Quien quiera, durante y en relación con cualquier violación de delito grave enumerada en la sección 2332b (g) (5) (B), transfiera, posea o use a sabiendas, sin autorización legal, un medio de identificación de otra persona o un documento de identificación falso deberá, Además de la pena prevista para tal delito grave, ser condenado a una pena de prisión de 5 años.

Fraude por cable, radio o televisión, Titulo 18 U.S. Código § 1343

Este código establece que:

Quien 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 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, La Ley de Asistencia de Emergencia y Ayuda por Desastres, 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.

Atentado de Conspiración, Titulo 18 U.S. Código § 1349

Este código establece que:

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.

Tratas de bienes y servicios falsificados, Titulo 18 U.S. Código § 2320 (a)(1)

Este código establece que:

Quien intencionalmente trafica bienes o servicios utilizando una marca falsificada en dichos bienes o servicios en relación con ellos.

(A) Recibe una multa no más de $ 2,000,000 o encarcelado no más de 10 años. Si no un era individuo debe recibir una multa de no más de $ 5,000,000.

(B) Por una segunda ofensa debe ser multado por no más de $ 5,000,000 o encarcelado no más de 20 años. Si no es un individuo, debe ser multado no más de $ 15,000,000.

Lavado de instrumentos monetarios, Titulo 18 US Código § 1956:

Este código establece que:

El término "institución financiera" incluye a cualquier persona que conspire para cometer cualquier delito definido en esta sección o sección 1957 estará sujeto a las mismas sanciones que las prescritas para el delito cuya comisión fue objeto de la conspiración. Le dan una pena civil si los daños no se pasan de los $10,000.

Casos Relacionados

Caso #1: USA vs Fabio Gasperini, No. Case 16-CR-441.

Según United States Department of Justice (21 de abril de 2017), el Tribunal Federal de Brooklyn acusó a Fabio Gasperini la creación de una red de bots global y la perpetración de un fraude en el que bots para imitar "clics" en publicidad de sitios web y obtener ingresos publicitarios. Los cargos incluyen intrusión informática, wire fraud conspiracy, wire fraud y lavado de dinero. Fue arrestado en Amsterdam en Paises Bajos, el 18 de juniode 2016. Gasperini. hackeó secretamente servidores informáticos de compañías e individuos en los Estados Unidos y en otros lugares. Creó una puerta trasera exclusiva que le permitió acceder a los datos y al poder de cómputo de esos servidores. A través de su puerta trasera, Gasperini implantó software malicioso en los servidores comprometidos. El software malicioso sirvió para propagar aún más el esquema de Gasperini al escanear el internet e identificar servidores vulnerables adicionales para la infección, lo que le permite crear una red de bots, una red de computadoras (como servidores) infectadas con software malicioso sin el conocimiento de los usuarios de que un actor malicioso puede tener control remoto y uso con fines maliciosos.

Un fraude de clics es un tipo de delito cibernético en el que un actor malintencionado obtiene dinero de manera fraudulenta de empresas y particularmente de empresas de publicidad. Tenía servidores de computadoras en todo el mundo, pero también utilizo dichos servidores en Estados Unidos. Parte del Software malicioso que Gasperini instalo fue creado para disfrazar un servidor comprometido como un navegador web y provocar que simule clics humanos en anuncios de sitios web a través de comandos electrónicos automatizados. Se encargaba de enviar clics automáticos a anuncios alojados en sitios web de propiedad, lo que le permitió a Gasperini generar ingresos de compañías y empresas de publicidad a través del tráfico de internet falso.

Los cargos en la acusación formal son alegatos, y el acusado se presume inocente hasta que se pruebe su culpabilidad. El caso del Gobierno está siendo procesado por la Oficina de Sección de Seguridad Nacional y Ciberdelincuencia.

Caso #2 USA vs Solomon Oyesanya, No. Caso 1:16-cr-90.

Según United States Department of Justice (15 de julio de 2015), Solomon Oyesanya fue sentenciado a 27 meses de prisión por estafar a los contratistas de defensa de los Estados Unidos por conspiración para cometer fraude electrónico, y un término concurrente de 60 meses de prisión por cometer fraude bancario y robo de identidad agravado en relación con un plan para defraudar a TD Bank en el Distrito del Este de Virginia y el Distrito del Este de Pensilvania. Oyesanya también recibió la orden de cumplir un total de cinco años de libertad supervisada, perder $ 25,000 en ganancias criminales y pagar restitución a sus víctimas. El 28 de marzo, Oyesanya se declaró culpable de conspiración por cometer fraude electrónico en relación con un plan para estafar a los contratistas de defensa de los Estados Unidos. Fue parte de una conspiración, dirigida por dos ciudadanos nigerianos, para obtener de manera fraudulenta hardware y productos de computadoras de contratistas y proveedores que fueron aprobados para hacer negocios con el gobierno de los EE. UU., específicamente el Departamento de Defensa de los EE. UU. Para lograr este esquema, los miembros de la conspiración crearon sitios web y cuentas de correo electrónico falsos de los EE. UU. Colocaron órdenes de compra gubernamentales fraudulentas con contratistas y proveedores sobre grandes cantidades de hardware para computadoras y productos similares.

A base de los documentos judiciales, las víctimas de los contratistas de defensa sufrieron pérdidas reales atribuibles a Oyesanya en exceso de $160,000 y pérdidas previstas atribuibles en exceso de $ 970,000. Oyesanya y sus co-conspiradores obtuvieron acceso a las cuentas de los

clientes legítimos de TD Bank mediante el uso de la identificación legítima de los clientes, como sus nombres, las fechas de nacimiento, las direcciones y números de seguro social, así como las licencias de conducir falsificadas. Oyesanya y sus co-conspiradores hicieron depósitos en forma de cheques falsificados, pequeñas cantidades de efectivo en las cuentas de clientes existentes de TD Bank para obtener información de la cuenta o, si se trata de un cheque fraudulento, para retirar fondos antes de que TD Bank descubriera que el cheque era fraudulento. También obtuvieron acceso en línea a las cuentas de clientes, así como acceso a nuevas tarjetas de débito de cajeros automáticos y números PIN en los nombres de los clientes existentes de TD Bank. Como resultado de este esquema, TD Bank sufrió pérdidas reales que superaron los $ 500,000 y las pérdidas previstas superaron los $ 760,000.

Caso #3 USA vs Timothy Livingston, NO. Caso No. 15-cr-00626.

Según United States Department of Justice (16 de febrero de 2017), Timothy Livingston, 31, fue condenado en un esquema de piratería informática y robo de identidad que secuestró cuentas de correo electrónico de clientes para enviar correos electrónicos masivos no solicitados o "spam" y generó más de $ 1.3 millones en ganancias ilegales. Además, se declaró culpable de un cargo de conspiración para cometer fraude en conexión con computadoras y dispositivos de acceso, conspiración para cometer fraude en relación con correo electrónico y robo de identidad con agravantes. Livingston operaba en *Whole Lot of Nothing* LLC, una empresa especializada en el envío de correos electrónicos no deseados en nombre de sus clientes. Los clientes de Livingston incluían negocios legítimos, como compañías de seguros que deseaban enviar correos electrónicos masivos para anunciar sus negocios, así como entidades ilegales, como farmacias en línea que vendían narcóticos sin recetas. También utilizó servidores proxy y botnets para permanecer en el anonimato y evadir las técnicas de bloqueo de spam. El admitió además que

hackeó cuentas de correo electrónico individuales y utilizó servidores de correo corporativo para promover sus campañas de spam, lo que le permitió enviar grandes cantidades de spam sin identificarse como remitente. La División Cibernética del FBI investigó el caso. El abogado litigante principal William Hall Jr. de la Sección de delitos informáticos y propiedad intelectual, el fiscal federal adjunto Daniel Shapiro de la sección de piratería informática y propiedad intelectual del distrito de Nueva Jersey de la Unidad de delitos económicos y la fiscal federal adjunta Sarah Devlin de la Unidad de Lavado de Dinero por perdidas de activos enjuició el caso.

Herramientas de Investigación

Las herramientas de investigación es el mecanismo que ayuda a las autoridades a esclarecer los casos criminales que enfrenta a diario la humanidad. A través de ellas se obtiene conclusiones concretas donde pone fin al crimen realizado. De acuerdo con el National Institute of Standars and Technology (2006) en su guía "Integrating Forensic Techniques into Incident Response", para que se ejecute un buen proceso de análisis forense se realizan las fases de recolección, examinación, análisis e informe de hallazgos.

VMware – es el software de virtualización donde instalará bajo sistema operativo Windows 7 y todas las aplicaciones para realizar el análisis.

XAMPP Parental Control – es un servidor independiente de plataforma de codigo libre. Permite instalar de forma sencilla Apache en tu propio ordenador, sin importar tu sistema operativo ya sea, Linux, Mac, Windows o Solaris. Además, tiene servidores de bases de datos como SQL y SQLite con sus respectivos gestores phpMyAdmin y phpSQLiteAdmin. Incorpora intérpretes como PHP, Perl, servidores FTP como ProFTP o FileZilla FTP Serve, etc, (Mikoluk,2013).

Kali Linux –es la herramienta eficaz para la auditoria de redes y seguridad de la informática en general. Es la herramienta perfecta para hackers, que buscan los límites y fisuras en la seguridad de las redes y sistemas informáticos. Esto no está orientado a cometer actos ilegales, ya que ser hacker no está vinculado a la ciberdelincuencia, aunque algunos puedan dedicarse a utilizar sus conocimientos para cometer delitos (Rubén Andrés, 2016).

FTK – Forensic Tool Kit – es una plataforma forense digital mayormente utilizada por la corte, que permitirá la extracción de una imagen creyente y exacta de la información de los equipos digitales incautados, sin alterar en ninguna disposición el contenido de este. Esta herramienta tiene la capacidad de procesar, indexar, transpirar datos más seguidos y analizados (Access data, 2017, Carril Ramos, 2018).

SECCION III. SIMULACION

La simulación sobre los hechos es la clave principal en una investigación de caso por algún tipo de fraude presentado. Recrea la escena del crimen y los pasos que los atacantes utilizaron para afectar a las víctimas. Es uno de los recursos más usado y confiable. Además, le provee a los investigadores y las agencias de ley y orden, la comprensión y conceptualización de los inicios de los actos conducidos por los criminales cibernéticos hasta cumplir los hechos delictivos. En el caso de USA vs Bogdan Nicolescu, Radu Miclaus y Tiberiu Danes trata sobre una conspiración de fraude de robo de identidad, lavado de dinero y criptominio realizado en los Estados Unidos cuyo fraude abarcó en unos 4 millones de dólares. El grupo de Bayrob así fue nombrada la conspiración por sus propios administradores cuando comenzaron a realizar su felonía.

Diagrama de simulación de fraude

Bogdan Nicolescu, Tiberiu Danet y Radu Miclaus fueron parte de una conspiración de fraude hacia los usuarios en la web. La sede principal del grupo Bayrob estaba localizada en Rumania. Los pasos que utilizaron para engañar a las víctimas fue de manera fácil y precisa donde por un enlace de correo electrónico malicioso que pretendían ser legítimos de entidades como Western Union, Norton AntiVirus y el IRS cuyo contenido era un malware nombrado el troyano Bayrob, ya sea enviándolo por las redes sociales, tiendas virtuales o por cualquier otro punto estratégico en la web que no tuviera protección, obteniendo así su información personal, números de tarjetas de créditos y números de cuentas bancarias de los afectados. Cuando los destinatarios hacían clic en un archivo adjunto, el malware se instalaba ocultamente en su computadora. El método que ellos utilizaban para tener comunicación de Rumania a Estados Unidos era a través de

servidores proxis. Cuando los usuarios entraban a la internet a realizar sus tareas era el punto clave para ellos atacar.

A continuación, se muestra un Diagrama donde presenta el orden de los pasos que los ciber criminales utilizaron para cometer su delito en la web.

Diagrama sobre los hechos ocurridos en el caso de USA vs Bogdan Nicolescu, Tiberiu Danet y Radu Miclaus:

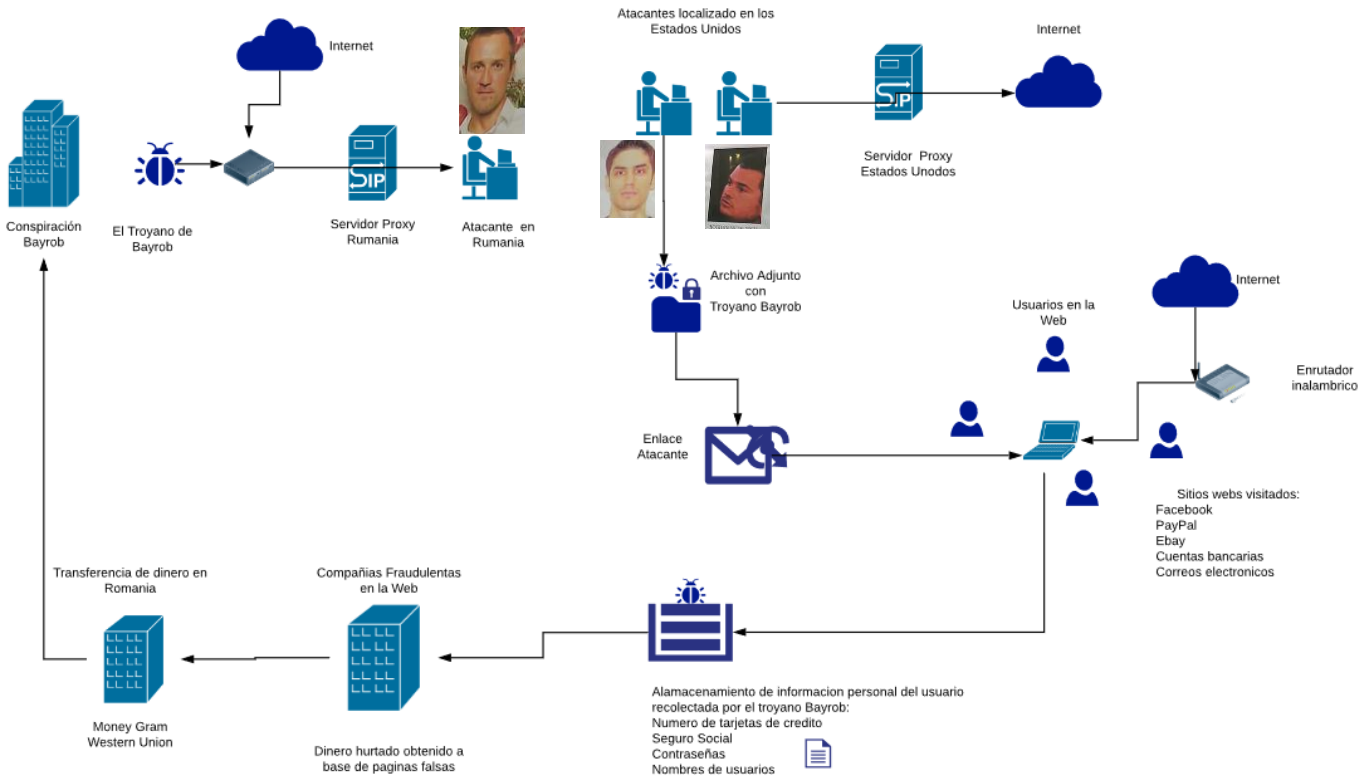
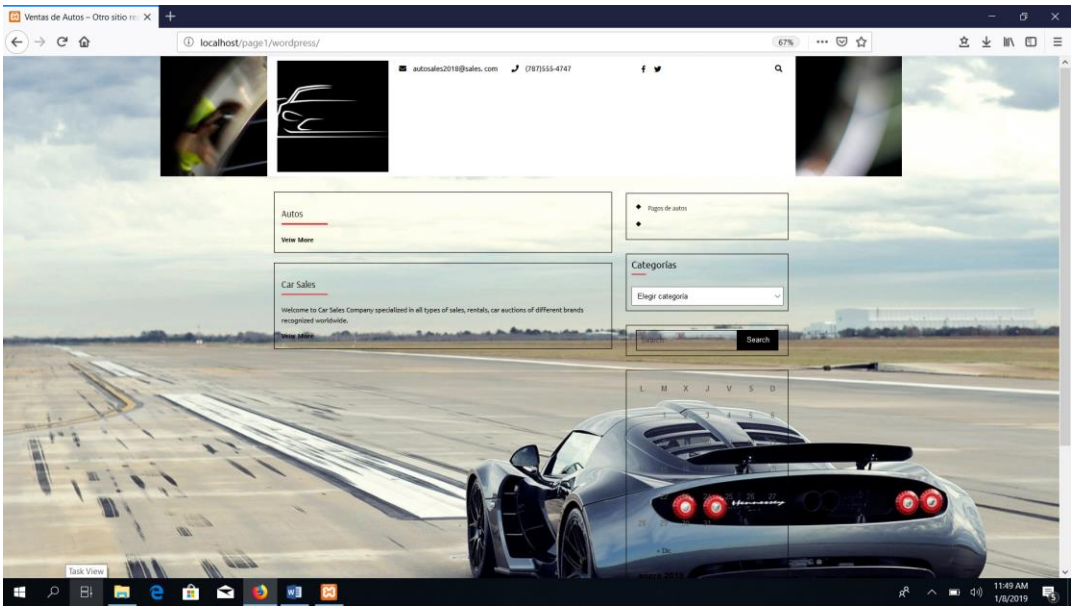


Figura 2: Esquema de fraude por parte de los acusados.

El diagrama del troyano de Bayrob nos mostró detalladamente como fueron sus pasos al cometer su felonía hacia las víctimas. Además, su proceso de función no era tan difícil, pero si muy peligrosa, debido a que no solamente obtenían la información, sino que hurtaban su dinero.

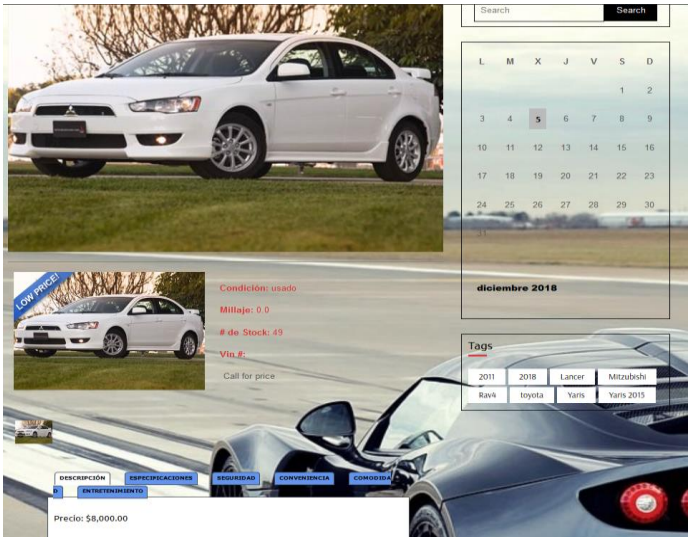
Por consiguiente, la mayor parte el dinero que ellos obtenían lo utilizaban para comprar servidor proxis de alto rango y espacio de almacenamiento adicional para guardar las informaciones robadas quienes eran manejados por los agentes contratados por la conspiración. Para culminar, su trabajo era de manera fantasma, esto significa que entre más lejos estuviera las paginas asociadas con la policía, más eficaz iba a ser su trabajo.

Página web falsa de los acusados donde realizaban sus esquemas de fraudes



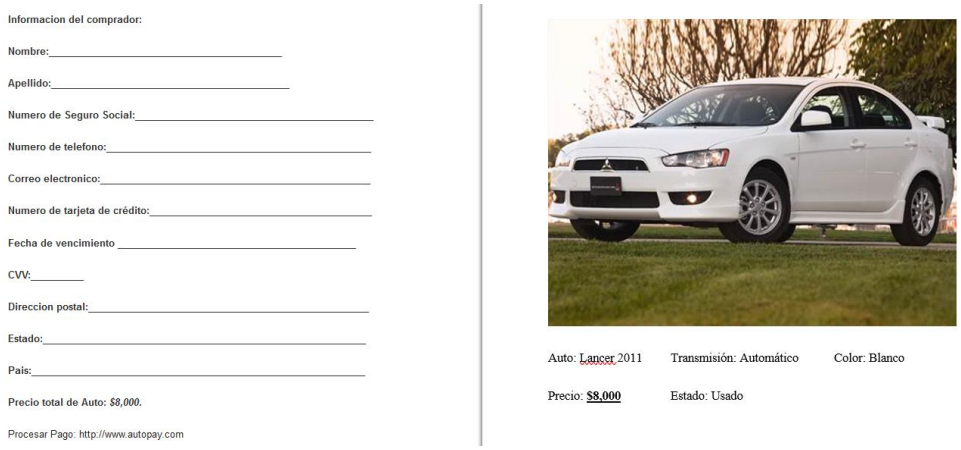
Véase figura 3: Página web falsa.

Auto seleccionado por la victima que su valor fue de $8,000.00.



Véase figura 4: Auto seleccionado por la victima

Documento para la entrada de información del comprador.



Informacion del comprador:

Nombre:_____

Apellido:_____

Numero de Seguro Social:_____

Numero de telefono:_____

Correo electronico:_____

Numero de tarjeta de crédito:_____

Fecha de vencimiento _____

CVV:_____

Direccion postal:_____

Estado:_____

País:_____

Precio total de Auto: ***$8,000.***

Procesar Pago: http://www.autopay.com

Auto: Lancer 2011 Transmisión: Automático Color: Blanco

Precio: **$8,000** Estado: Usado

Figura 5: Documento para proceso de pago del auto.

SECCION IV. INFORME DEL CASO

Resumen Ejecutivo

En relación con el caso de United State of America vs Bogdan Nicolescu, Tiberiu Danet, Radu Miclaus, Nicole S. Rendon y el Negociado Federal de Investigaciones le entregaron a JRS Information Security un USB con una copia disco duro de la computadora de la víctima. La evidencia recolectada será el objetivo principal del caso para ser sometida a un análisis forense. Ademas, la evidencia recolectada por el FBI será sometida a una serie de pruebas con las herramientas de altos estándares en la industria, para garantizar que el análisis sea preciso y levante evidencia necesaria de como los acusados cometieron su delito. La información obtenida del proceso de análisis servirá como prueba integra para sostener el caso ante el Tribunal de Justicia Federal.

Objetivo

El Departamento de Justicia y su corte de Distrito de Ohio contrata los servicios de JRS Information Security con el objetivo de identificar, analizar y recuperar la evidencia adquirida por el Negociado Federal de Investigaciones en la evidencia incautada. Esto es con el propósito y enfoque de obtener material que evidencie y confirme las acusaciones imputadas a los acusados. JRS Information Security cumple con los equipos adecuados para incautar toda la información necesaria y presentar su evidencia ante la justicia.

Alcance del trabajo

Los investigadores y el FBI le hacen entrega a Jose Ramos Soto, Investigador de Seguridad de la información de JRS Information Security un USB con la imagen del disco duro de la computadora incautada. Esta pieza fue entregada por el FBI con el propósito de analizar y adquirir la evidencia exacta del crimen cometido ya que a través de ella se tiene información de alto valor. Fue la pieza clave para que las autoridades tomaran acción e investigaran a los atacantes sobre el caso de United State of America vs Bogdan Nicolescu, Tiberiu Danet, Radu Miclaus. La compañía JRS Information Security se le ha

indicado la labor de adquirir, mantener, y descubrir evidencia en el equipo electrónico con el fin de analizarlo para ser presentado como evidencia al fiscal Carole S. Rendon. JRS Information Security en seguimiento con los estándares expuesto dentro de la industria de seguridad de información, comienza el proceso de análisis utilizando los siguientes equipos de seguridad:

- ✓ Ordenadores virtuales – *Windows 7 Professional*

Datos del caso:

Numero de caso: 1:16-cr0024

Caso: United State of America Vs. Bogdan Nicolescu, Tiberiu Danet, y Radu Miclaus

Violación: 18 U.S. Código § 1343

Acusado: Bogdan Nicolescu

Acusado: Tiberiu Danet

Acusado: Radu Miclaus

Investigador: Jose Ramos Soto

Cliente: FBI

Representante: Carole S. Rendon (Fiscal)

Descripción de los equipos utilizados

En JRS Information Security cuenta con el mejor equipo de análisis forense donde tomara datos de la evidencia incautada por el FBI. Además, cumple con un alto rango de estándares dentro de la compañía de análisis forense digital.

Computadora portátil Asus, color negro, modelo UX4104A

Figura 6: Ordenador portátil.

Encontraron USB Flashdrive, color negro de 8gb, conteniendo la imagen de disco duro.

Figura 7: USB Flashdrive.

Resumen de los hallazgos

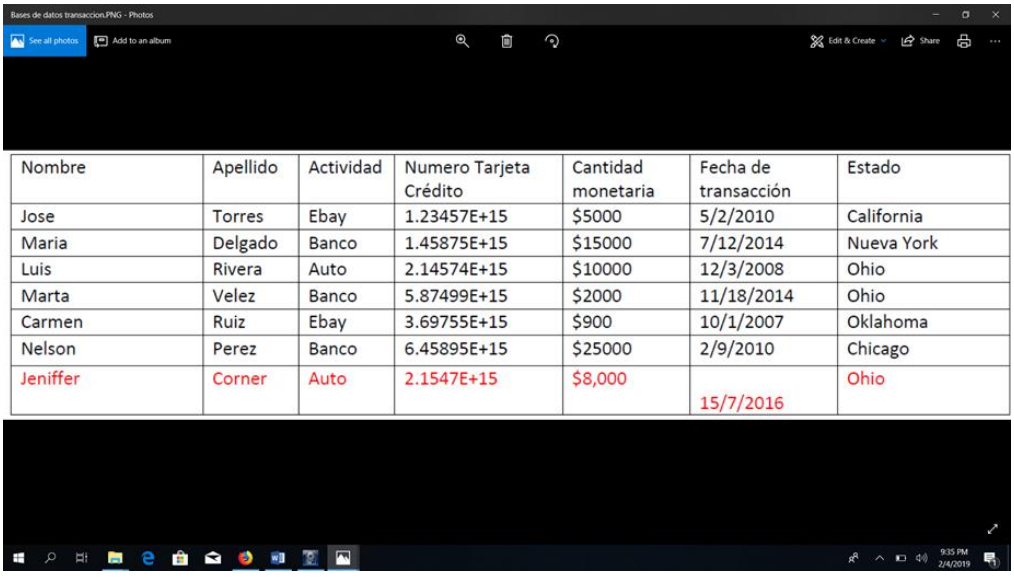
Después de que JRS Information Security realizara el proceso de investigación y toma de datos de forma rigurosa del dispositivo incautado, se encontraron documentos de una base de datos que contenían información confidencial de las víctimas y los tipos de transacciones que los atacantes realizaron. Además, se obtuvo una imagen donde muestra la confirmación de pago que la víctima proceso. Por consiguiente, estos documentos fueron analizados con el mismo fin de exponer a los acusados como responsables en su totalidad del delito que el FBI y el Departamento de Justicia le imputa haber cometido. Los procesos aplicados serán mostrados en las próximas figuras expuestas.

Documento de una base de datos con la información completa de los números de tarjetas de créditos.

Nombre	Apellido	Número de Seguro Social	Banco	Número de cuenta	Numero Tarjeta Crédito	Código seguridad	Cantidad monetaria	Email
Jose	Torres	555-87-6969	PNC Bank	545858478	1.23457E+15	252	5,000.00	jose.torres@live.com
Maria	Delgado	2147-65-987	U.S.Bank	236974589	1.45875E+15	694	15,000.00	maria.delgado@hotmail.com
Luis	Rivera	787-20-8584	Bank of America	235424789	2.14574E+15	363	10,000.00	luis.perez@hotmail.com
Marta	Velez	525-10-3247	PNC Bank	542156987	5.87499E+15	545	2,000.00	marta.velez@yahoo.com
Carmen	Ruiz	212-32-2325	U.S.Bank	102300248	3.69755E+15	987	900.00	carmen.ruiz@gmail.com
Nelson	Perez	202-36-7474	Bank of America	254874478	6.45895E+15	989	25,000.00	nelson.perz@live.com
Jeniffer	Corner	584-65-9874	Bank of America	546987549	2.1547E+15	541	8,000.00	jeniffercorner12@gmail.com

Figura 8: Hallazgo de base de datos de tarjetas de créditos.

Documento de una base de datos con las informaciones de las transacciones realizadas por los atacantes.



Nombre	Apellido	Actividad	Numero Tarjeta Crédito	Cantidad monetaria	Fecha de transacción	Estado
Jose	Torres	Ebay	1.23457E+15	$5000	5/2/2010	California
Maria	Delgado	Banco	1.45875E+15	$15000	7/12/2014	Nueva York
Luis	Rivera	Auto	2.14574E+15	$10000	12/3/2008	Ohio
Marta	Velez	Banco	5.87499E+15	$2000	11/18/2014	Ohio
Carmen	Ruiz	Ebay	3.69755E+15	$900	10/1/2007	Oklahoma
Nelson	Perez	Banco	6.45895E+15	$25000	2/9/2010	Chicago
Jeniffer	Corner	Auto	2.1547E+15	$8,000	15/7/2016	Ohio

Figura 9: Hallazgo de base de datos de transacciones realizadas.

Documento de una captura de imagen sobre la confirmación de pago enviada al correo electrónico

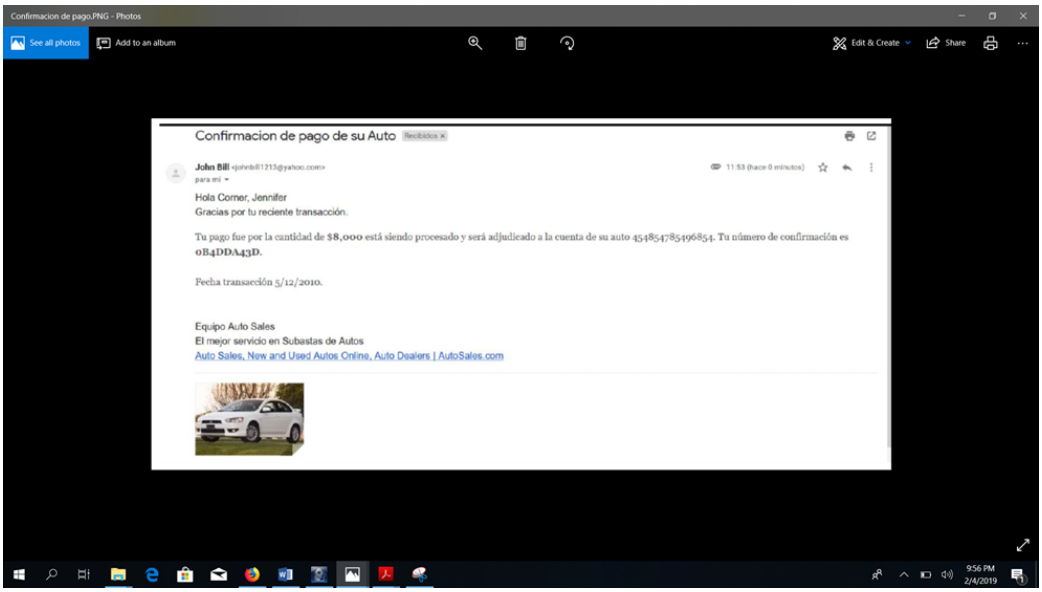


Figura 10: Hallazgo confirmación de pago.

Cadena de custodia:

La cadena de custodia es el procedimiento establecido para documentar la historia cronológica de las muestras recogidas hasta su devolución, conservación o destrucción, con la finalidad de garantizar la integridad y autenticidad de las muestras y evitar, por tanto, su alteración, contaminación, sustitución o indebida manipulación (Fernandez de Simon Lourdes, 2013).

Detalles de la cadena de custodia

A continuación, se muestra a detalles los procesos de recolección de evidencia por JRS Information Security sobre la pieza de evidencia de una imagen del USB Flashdrive color negro de 8gb, relacionado al caso de investigacion United State of America vs. Bogdan Nicolescu, Tiberiu Danet, Radu Miclaus.

PRIMER EVENTO

Evidencia recogida por: Jose Ramos Soto

Fecha: 15 de septiembre de 2007

Hora: 10:00 am

Agencia: JRS Information Security

Evidencia entregada por: Nicole S. Rendon

Agencia: Negociado Federal de Investigaciones (FBI)

Lugar de recogido: Deposito del FBI

Destino de la entrega: Laboratorio de investigación de JRS Information Security

Números de piezas de evidencia: 1

Descripción física: USB Flashdrive color negro 8gb.

Propósito: Análisis forense del contenido del dispositivo.

SEGUNDO EVENTO

Evento: Análisis de la pieza de la evidencia.

Agencia: JRS Information Security

Evento verificado por: Jose Ramos Soto

Lugar de análisis: Laboratorio de investigación de JRS Information Security.

Número de piezas de la evidencia: 1

Descripción física: USB Flashdrive color negro 8gb.

Hora: 8:00 am

Fecha de Terminación 16 de septiembre del 2007.

Hora: 7:00 pm.

TERCER EVENTO

Evidencia recogida por: Nicole S. Rendon.

Agencia: FBI.

Evidencia entregada por: Jose Ramos Soto.

Agencia: JRS Information Security.

Lugar de recogido: Laboratorio de investigaciones de JRS Information Security.

Hora: 8:00 pm.

Destino de la evidencia: Deposito del FBI del estado de Ohio.

Número de piezas: 1.

Descripción física: USB Flashdrive color negro 8gb.

Propósito: Devolución de las piezas de la evidencia debidamente analizadas.

Procedimiento

Una vez entregada la pieza de la evidencia a JRS Information Security se prepara la misma para el proceso de análisis forense. Además, para cumplir con los estándares de análisis forense digital se utilizarán las herramientas de FTK, que permite crear una copia fiel y exacta de los datos sin alterar, modificar la evidencia real. La evidencia real será almacenada en un lugar seguro para ser protegido de daños accidentales o intencionales mientras se lleva a cabo la investigación. Luego que el FBI le hace entrega la pieza incautada a los expertos de JRS Information Security para realizar el análisis forense, así tomado evidencia sobre el caso.

Programa para correr ordenador virtual con el sistema operativo Windows 7 Professional

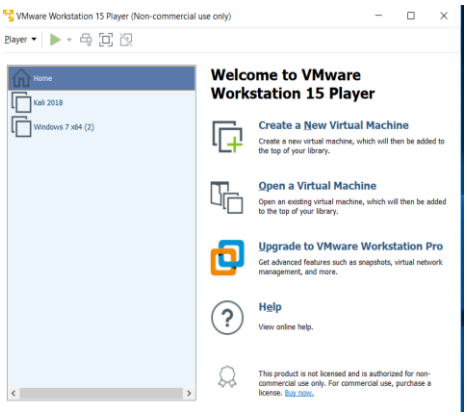


Figura 11: Programa VMware

Ordenador virtual Windows 7 en VMware instalado y en ejecución.

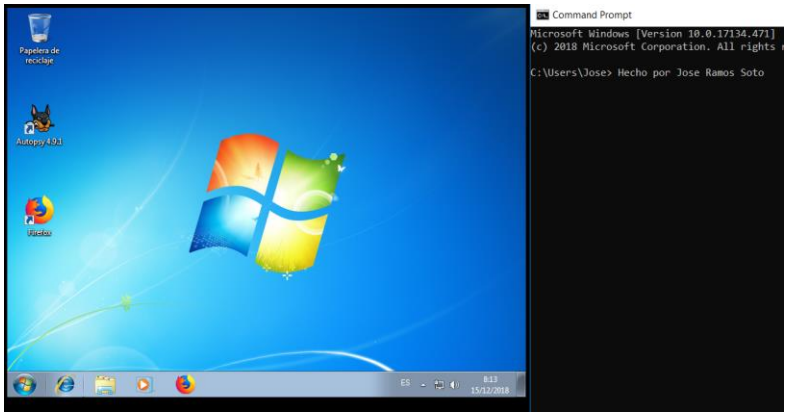
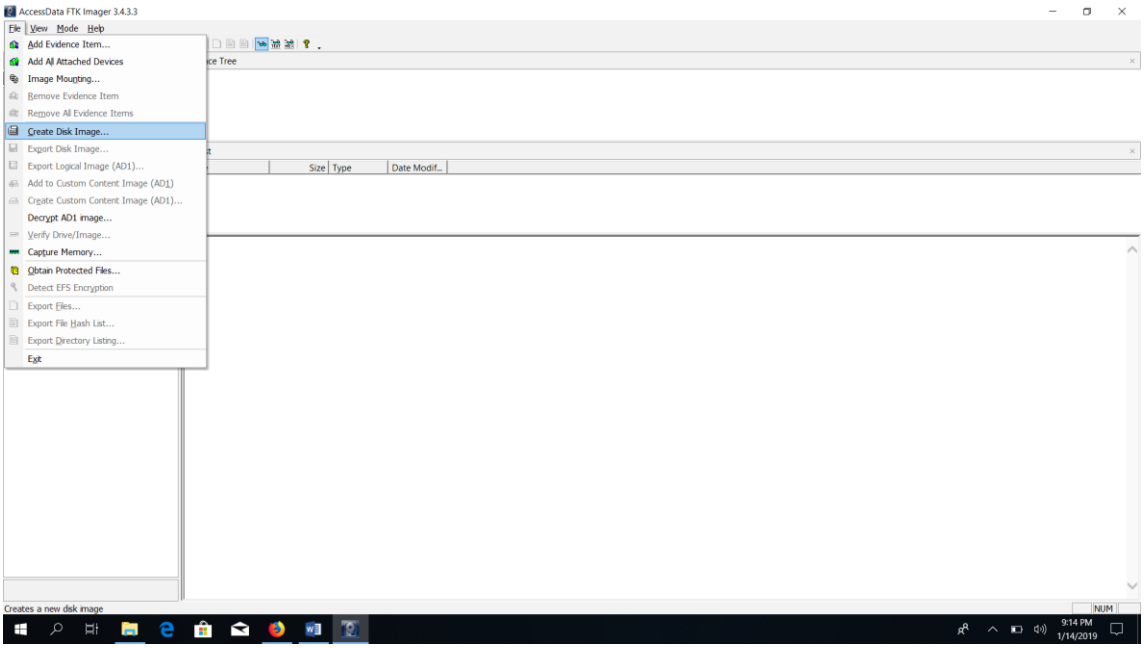


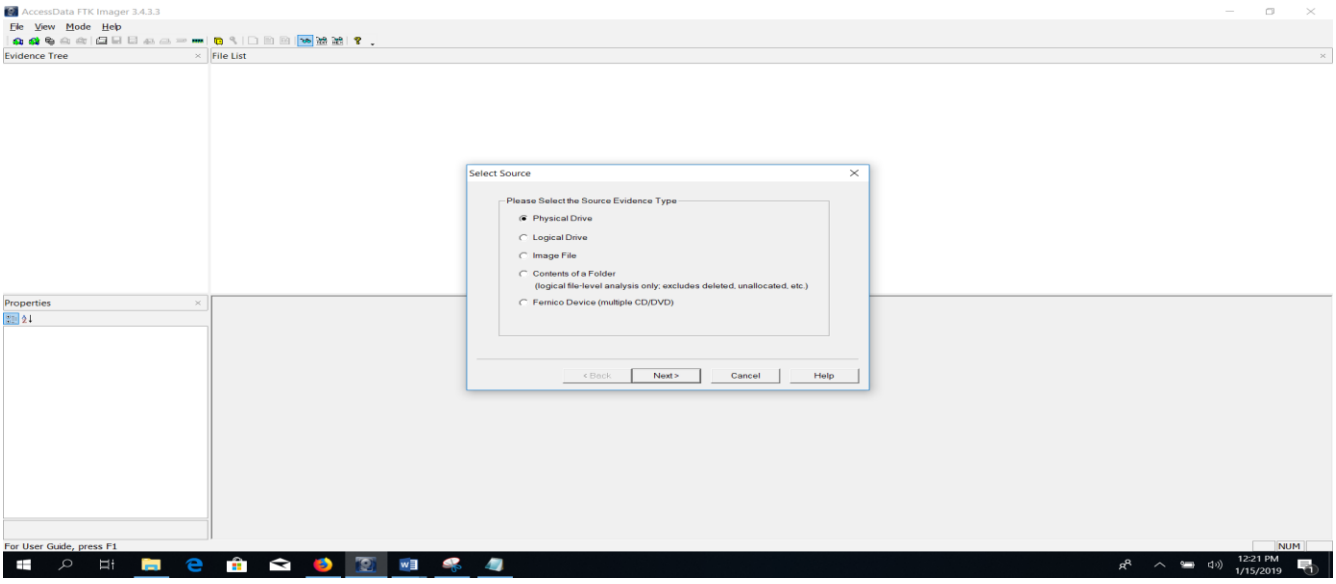
Figura 12: Ejecución de ordenador virtual

Programa forense FTK Imager Acess Data para el análisis de evidencia capturada desde la imagen de disco duro.



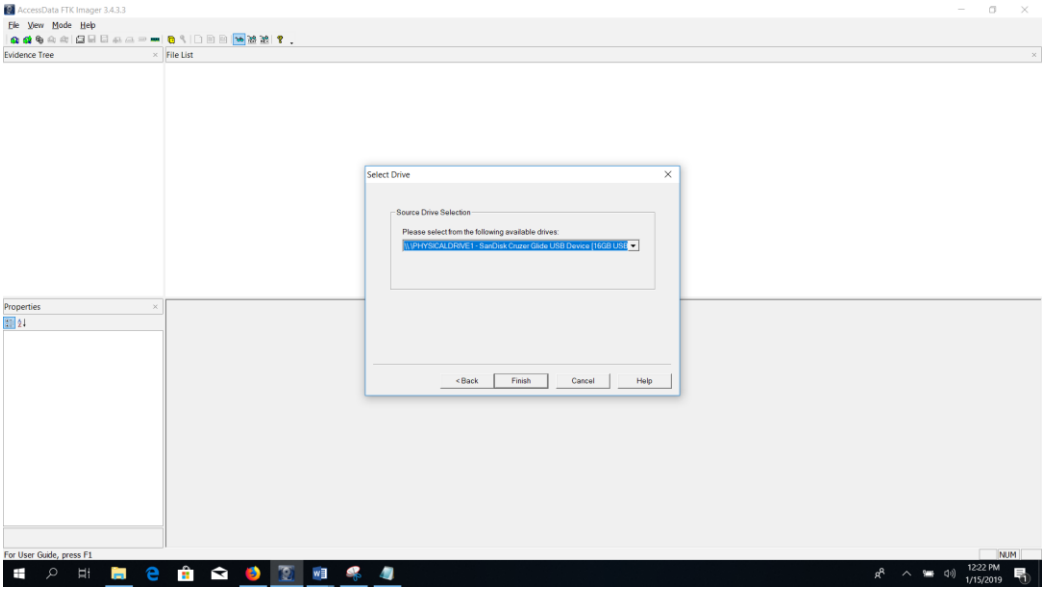
Véase la figura 13: Análisis de la unidad física

Desarrollo de evidencia dentro de la unidad física.



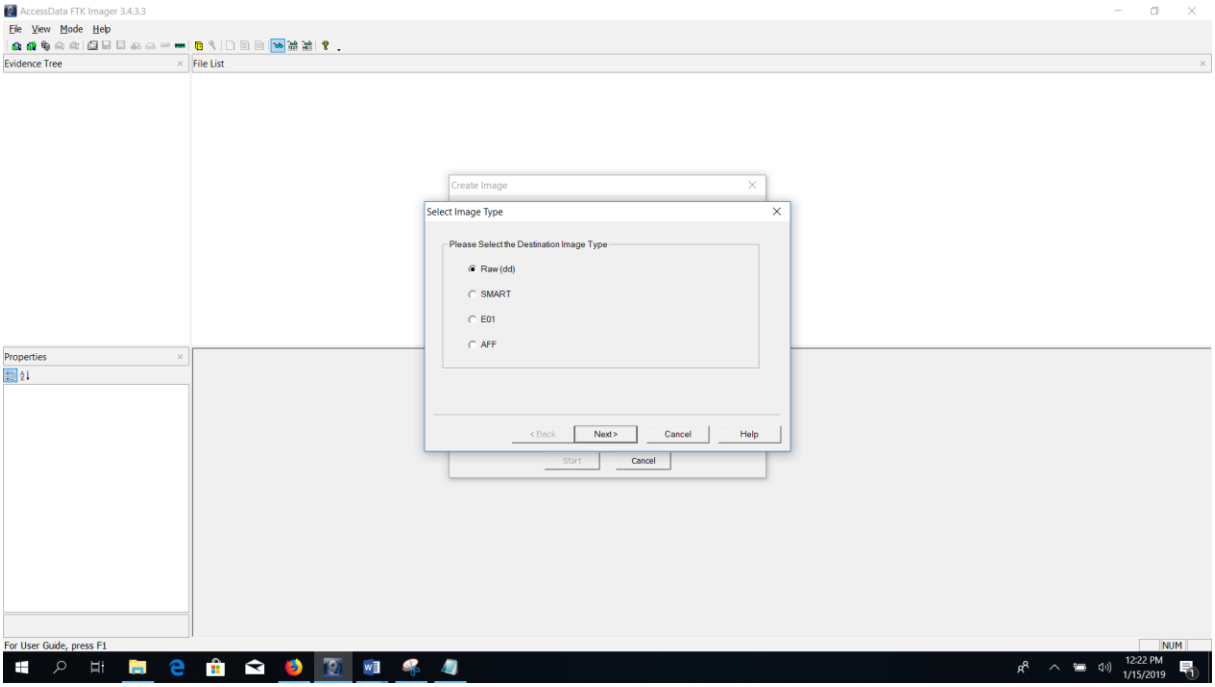
Véase la figura 14: Desarrollo de evidencia

Selección de la unidad física que será analizada.



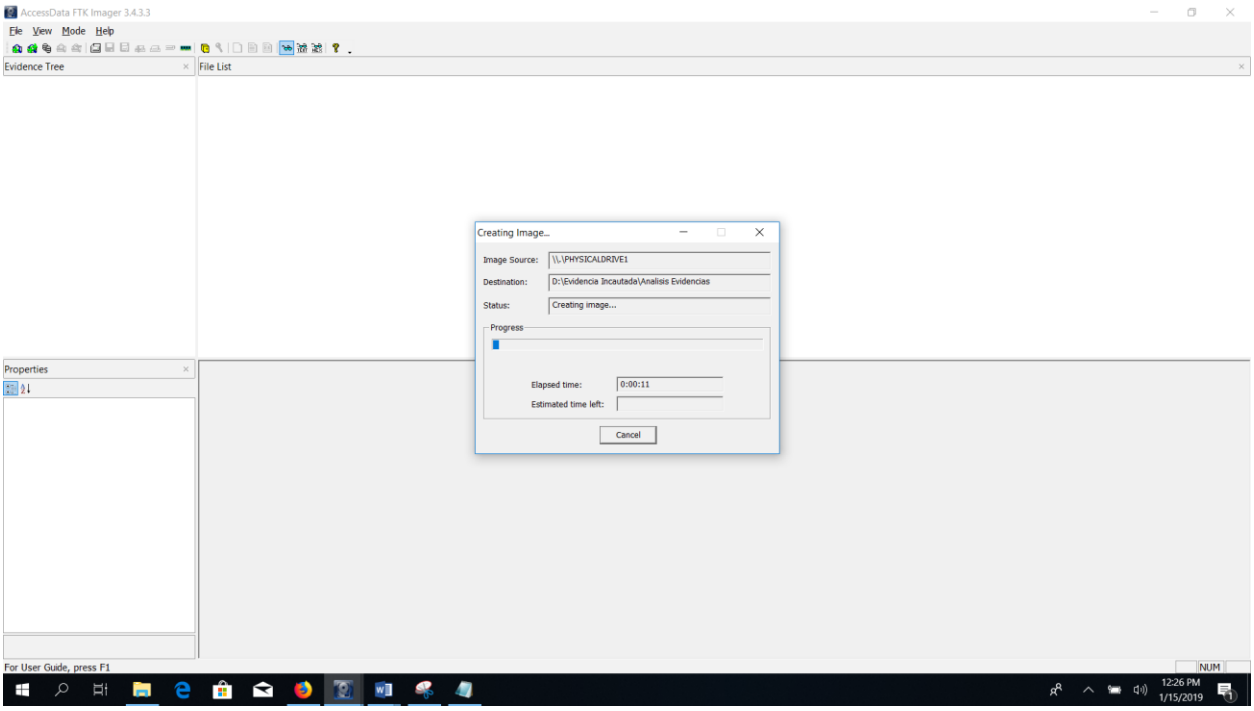
Véase figura 15: Selección unidad física.

Conversión de la imagen EVE a DD.



Véase la figura 16: Conversión de EVE a DD.

Progreso del proceso de analisis para la obtencion de la evidencia por parte de la unidad fisica.



Vease la imagen 17: Progreso de evidencia.

Evidencia encontrada en la unidad física. Documentos de una base de datos y una imagen de confirmación de pago.

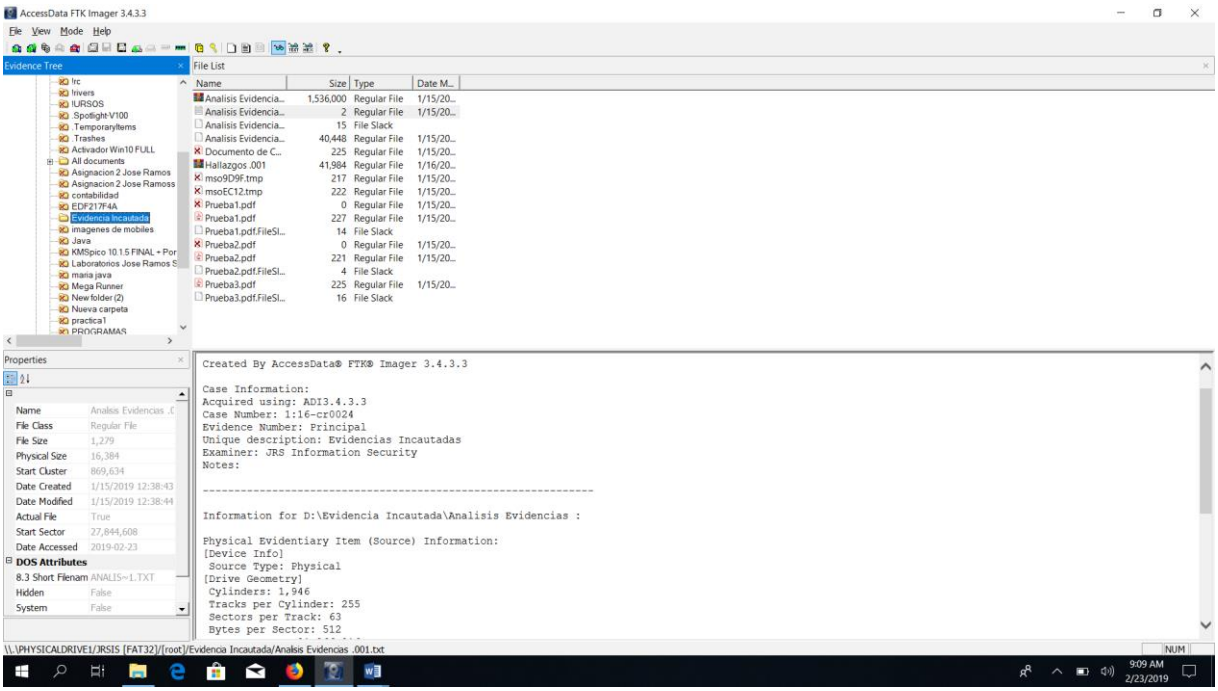
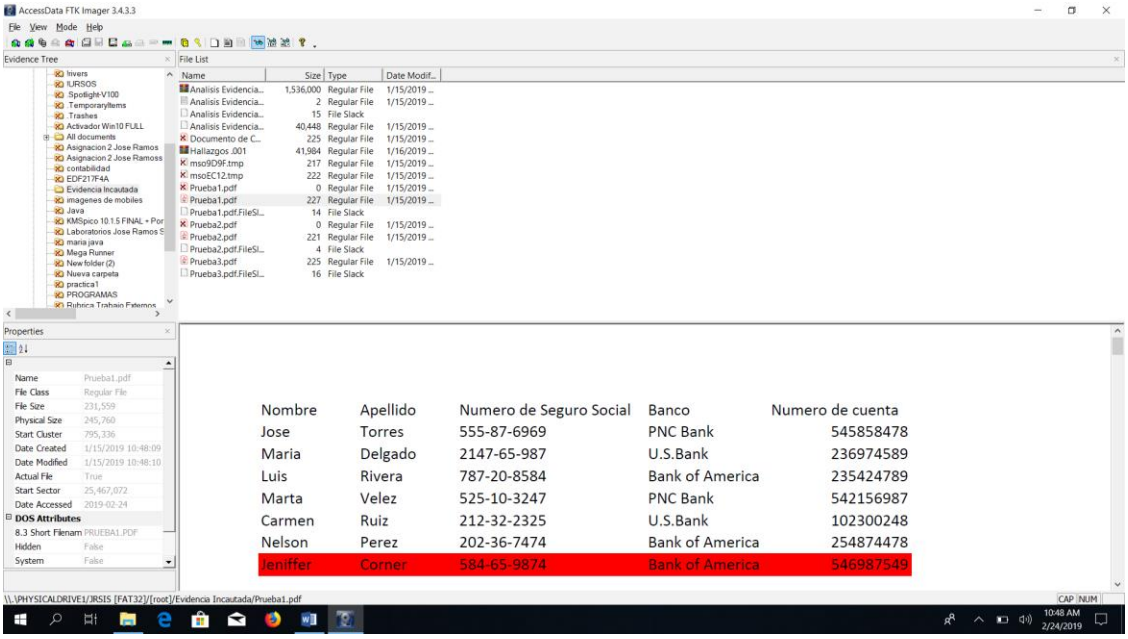


Figura 18: Evidencia encontrada

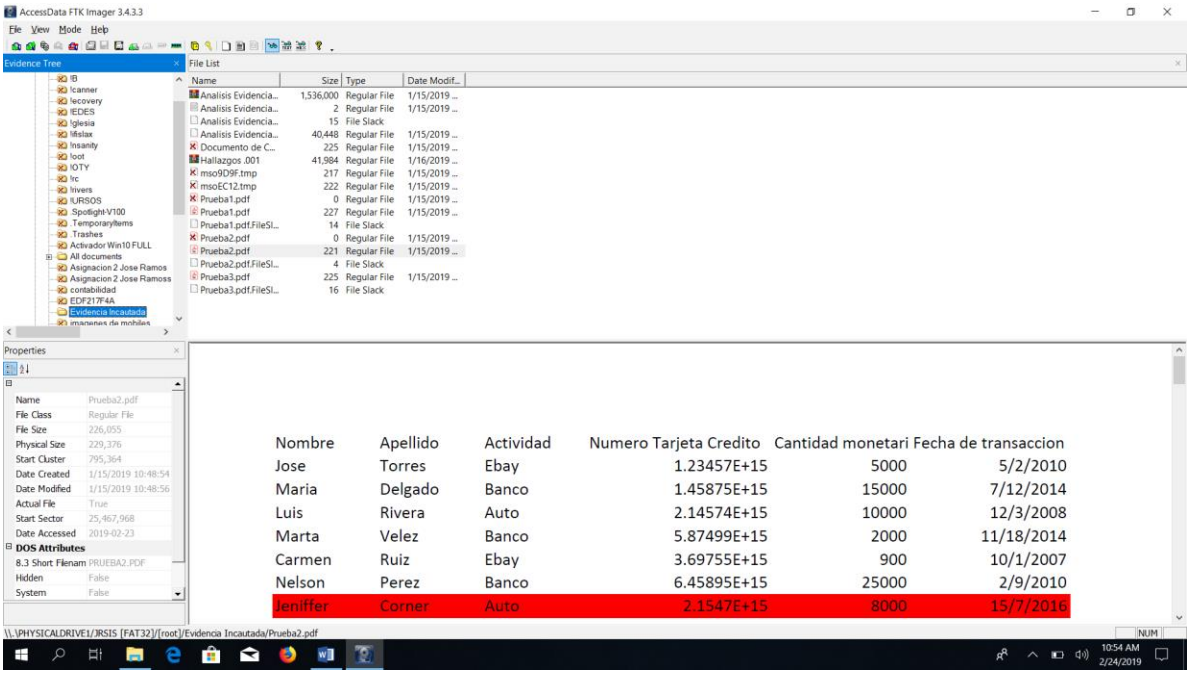
Docunento con informacion confidencial de las victimas y sus tarjetas de creditos.



Nombre	Apellido	Numero de Seguro Social	Banco	Numero de cuenta
Jose	Torres	555-87-6969	PNC Bank	545858478
Maria	Delgado	2147-65-987	U.S.Bank	236974589
Luis	Rivera	787-20-8584	Bank of America	235424789
Marta	Velez	525-10-3247	PNC Bank	542156987
Carmen	Ruiz	212-32-2325	U.S.Bank	102300248
Nelson	Perez	202-36-7474	Bank of America	254874478
Jeniffer	Corner	584-65-9874	Bank of America	546987549

Figura 19: Documento con información de las tarjetas de créditos.

Documento con la informacion confidencial de las transacciones realizadas por los atacantes



Nombre	Apellido	Actividad	Numero Tarjeta Credito	Cantidad monetari	Fecha de transaccion
Jose	Torres	Ebay	1.23457E+15	5000	5/2/2010
Maria	Delgado	Banco	1.45875E+15	15000	7/12/2014
Luis	Rivera	Auto	2.14574E+15	10000	12/3/2008
Marta	Velez	Banco	5.87499E+15	2000	11/18/2014
Carmen	Ruiz	Ebay	3.69755E+15	900	10/1/2007
Nelson	Perez	Banco	6.45895E+15	25000	2/9/2010
Jeniffer	Corner	Auto	2.1547E+15	8000	15/7/2016

Figura 20: Documento con informacuones de sus transacciones.

Documento sobre captura de imagen de la confirmación de pago enviada por los atacantes.

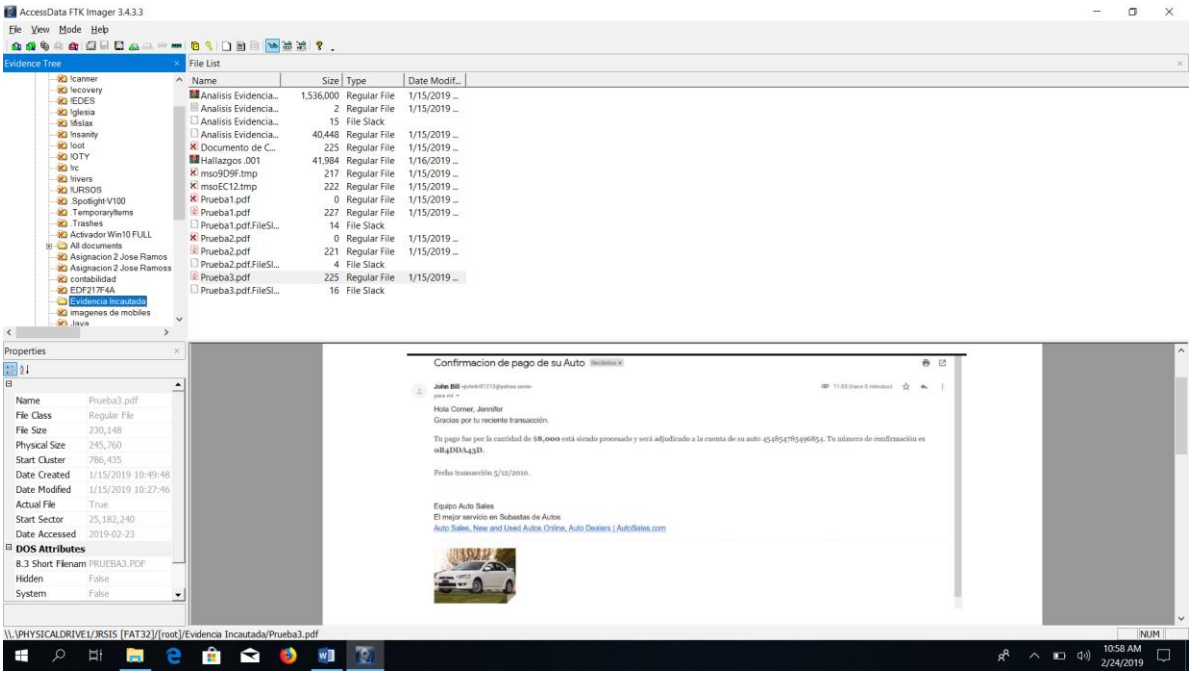


Figura 21: Confirmación de pago.

SECCION V. DISCUSION DEL CASO

Luego de haber finalizado el análisis de la información, contenida dentro del disco duro de la computadora incautada por los agentes del FBI almacenada en USB Flashdrive y entregada a JRS Information Security, se llega a la conclusión de que el Grupo Bayrob constituido por Bogdan Nicolescu, Radu Miclaus y Tiberius Danes organizaron varios esquemas de fraudes aprovechándose de los beneficios de las victimas afectadas, obteniendo en sí su dinero e información de alto valor.

Como método de observación del esquema de fraude por la Conspiración de Bayrob cumple en su totalidad en el triángulo del Fraude de Donald Cressey. Según expuesto en (Wells) el triángulo de Cressey se compone de 3 elementos: percepción, oportunidad percibida y racionalización. El primero es la percepción, es la presión que el grupo de Bayrob tenía para obtener el dinero de la víctima era su situación económica, ya que con la cantidad monetaria robada iban a continuar creciendo su infraestructura fraudulenta y pagar sus lujos personales. Para penetrar el fraude, la conspiración utilizó herramientas engañosas haciéndole saber a los usuarios que estaban navegando en páginas oficiales y confiables. Fue el momento preciso para entrar dentro de su ordenador y obtener los resultados esperado, que en este caso era robar toda la información confidencial del usuario. La oportunidad de los defraudadores para ejecutar su esquema de fraude era el conocimiento alto sobre los equipos utilizados para implantarlos. Uno de los programas utilizado fue el bob, encargado de entrar de manera fantasma al ordenador y ejecutar su trabajo a base de las especificaciones codificadas por ellos. La racionalización de esquema de fraude por el grupo Bayrob fue la intención de adquirir los fondos para sufragar sus necesidades.

Según se pudo verificar en los documentos del Departamento de Justicia del Distrito de Ohio los imputados fueron acusados de 21 cargos por esquemas de fraudes. Luego de analizar pausadamente la información contenida en el dispositivo incautado por el Negociado Federal de Investigaciones se

concluye que la información obtenida y analizada, se relacionan directamente con los acusados Bogdan Nicolescu, Radu Miclaus y Tiberius Danes con los delitos elaborados. Las imágenes obtenidas son evidentes y demuestran que por medio de los documentos generados con el conocimiento del grupo de Bayrob. Acordaron y organizaron la estrategia de someter paginas falsas y el peligroso troyano Bayrob a los ordenadores, logrando así la obtención de su dinero e información confidencial.

SECCION VI. AUDITORIA Y PREVENCION

En la actualidad el Internet es un método de comunicación global entre usuarios que ha ido evolucionando drásticamente. Entre más avanza la tecnología, más delitos cibernéticos pueden salir a la luz. La auditoría es la herramienta que se utiliza para ver los controles existentes dentro de diversos campos de trabajos y organizaciones. Tiene un pacto directo de forma positiva. Hoy día los usuarios al visitar la web están en un riesgo mayor de enfrentar el fraude. Además, al ingresar o crear algún tipo de cuenta ya sea de banco, tiendas virtuales, red social, etc., su información está expuesta a ser vandalizada por estos amenazantes. C existen controles que deberías aplicar para el buen manejo de la seguridad de la información. Contiene reglas que se tienen que cumplir para que todo opere eficazmente y permita la adopción de decisiones a su perfeccionamiento y mejora. Por ellos, la auditoria hace énfasis en sus principios de prevención, detección y corrección del buen manejo de la información en la web previniendo robos, fraudes y perdidas a usuarios activos.

Resumen de hallazgos

Durante el periodo de la investigación salieron a la luz los factores claves en el cual guiaron a los defraudadores a cometer su crimen cibernético. Como parte del conocimiento del atacante, nunca será descubierto su delito debido a su excelente trabajo, creando en él confianza. Por consiguiente, por un solo descuidos son descubiertos revelando así su esquema de fraude envuelto. Además, no tan solo esto, sino que también el peso de la ley y el orden caerá sobre ellos.

Los elementos efectuados por la conspiración fueron el desafío intelectual de destituir la ética y la información del personal. Los defraudadores al tener como objetivo la obtención de dinero mediante las directrices que le asignaban al troyano cuando entraba de manera fantasma por presionar un enlace o envió de correo electrónico a infectar cualquier equipo computarizado. Crearon medios de adecuados para engañar de forma intencionada a los usuarios. Esto refleja el nivel crítico de aprendizaje cuando se tiene acceso a la web. Además, no tan solo eso, sino las desventajas que pueden ocasionar. Las compañías que

se puede tener acceso a través de sus páginas virtuales tienen como objetivo principal la protección de información de sus usuarios.

Los controles por parte del usuario no fueron los correctos. La falta de conocimiento sobre los riesgos que se pueden enfrentar en la web es muy escasa. El fraude sucede segundo a segundo y minuto a minuto. La falta de ética y valores cada día va en decadencia, entre más avanzada la tecnología está más fácil va a ser el proceso para los hackers cometer su delito. Existen herramientas dentro del navegador que ayudan a evitar este tipo de amenazas. Por eso nunca exponga tu información personal en la web porque a la vez que lo intentes ya nada será igual.

Opinión de la auditoria

Luego del proceso de análisis detallado de la evidencia encontrada se convalida los procesos operacionales de la conspiración de Bayrob que no iban en cumplimientos de las regulaciones y las leyes que exigen el Gobierno Federal. Por la víctima no tener sabiduría completa de lo que estaba enfrentando al realizar su compra fue un punto clave para ser vulnerada afectando así su información personal y su dinero.

SECCION VII CONCLUSION

En el presente trabajo investigativo se planteó como objetivo principal analizar un caso sobre un esquema de fraude. Actualmente, el fraude es el villano más temido por muchos, mayormente las empresas. Existe una gama de controles y seguridad que se deben aplicar al realizar el análisis del caso.. Las herramientas permitieron crear y encontrar evidencia precisa para confirmar los delitos asignados a los culpables. Además, como parte del estudio, se creó una simulación que mostro el ambiente real del atacante realizando su plan maléfico. Los procesos efectuados permiten tener un control en la obtención de información confidencial, a base de las pruebas encontradas en el equipo incautado por las autoridades y agentes del Negociado Federal de Investigaciones.

El análisis del caso sobre varios esquemas de fraudes me permitió repasar los procesos realizados al hacer una investigación forense. Me brindó la oportunidad de reconocer documentos legales, programas de herramientas forenses y reforzar conocimientos previos sobre los controles que se deben aplicar cuando se tiene acceso a la web. Por consiguiente, permitió honrar el excelente trabajo que hacen los auditores y examinadores al detectar, documentar, esclarecer y prevenir escenarios de fraudes.Durante el periodo académico de la presente maestría en el campo de la seguridad de la información he recibido las herramientas y en la elaboración profesional activa de la prevención y detección del fraude. Para culminar, fue un placer ser parte de una asociación de investigación para la protección de la información de la Internet y prevención del fraude, donde adquirí un alto conocimiento como analista de fraude, para así en eventos futuros aplicarlos en el campo laboral.

SECCION VIII. REFERENCIAS

18 U.S.C § 371.Code - *Conspiracy to commit offense or to defraud United States.*

Legal Information Institute. Recuperado de

https://www.law.cornell.edu/uscode/text/18/371.

18 U.S.C § 1028A. *Aggravated identity theft. Legal Information Institute.*

Recuperado de https://www.law.cornell.edu/uscode/text/18/1028A.

18 U.S.C § 1349. *Attempt and conspiracy.* Legal Information Institute.

Recuperado de https://www.law.cornell.edu/uscode/text/18/1349.

18 U.S.C § 1343. *Fraud by wire, radio, or television.* Legal Information Institute

Recuperado de https://www.law.cornell.edu/uscode/text/18/1343.

18 USC. § 1956. *Laundering of monetary instruments.* Legal Information Institute

Recuperado de https://www.law.cornell.edu/uscode/text/18/1956.

18 U.S.C § 1028 (a)(1) y (2). *Fraud and related activity in connection with identification*

documents authentication features, and information. Legal Information

Institute.Recuperado de https://www.law.cornell.edu/uscode/text/18/1028A.

18 U.S.C. § 2320 (a)(1). *Trafficking in counterfeit goods or services.* Legal Information Institute.

Recuperado de https://www.law.cornell.edu/uscode/text/18/2320.

18 U.S.C § 2. *Principals.* Legal Information Institute. Recuperado de

https://www.law.cornell.edu/uscode/text/18/2.

Acurio Del Pino, S. (2016) Delitos Informáticos: Generalidades. Documento PDF. Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

Alcorn, W. (febrero 15,2014) *Beef Program*. Kali Tools. Recuperado de: https://tools.kali.org/exploitation-tools/beef-xss.

Arimetrica Digital, S.L con C.I.F. numero CIF B86181625 inscrita en el Registro Mercantil de Madrid, T 28670, F 195, S 8, H M 516332, I/A 1. Nuestro domicilio social se encuentra en C/ Juana Francés nº 12,2º (28320) Pinto. Recuperado de https://www.arimetrics.com/glosario-digital.

Brown, Cameron (febrero del 2013) Estudio Exhaustivo sobre el delito cibernético. Documento PDF de la Oficina de las Naciones Unidas contra la Droga y el Delito. Recuperado de https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf.

Carril Ramos, Z. (24 de noviembre de 2017) Forensinc Tool Kit. Documento PDF.

Cano C, M. A. (s.f) Fraude y Estafas en los Negocios. United States InterAmerican Community Affairs. Recuperado de http://interamerican-usa.com/articulos/Auditoria/Fraud-Estaf-Neg.htm.

Comisión Nacional Bancaria y de Valores (10 de septiembre de 2010) Lavado de dinero. Recuperado de https://www.cnbv.gob.mx/CNBV/Documents/VSPP_Lavado%20de%20Dinero.pdf.

Enciclopedia jurídica (n/a) Fraude. Recuperado de http://www.enciclopedia-juridica.biz14.com/d/fraude/fraude.htm.

Frolik, C. (30 de marzo de 2017). *Thousands in Ohio Fall Victim to Phishing Scam*. Government technology. Recuperado de http://www.govtech.com/security/Thousands-in-Ohio-Fell-Victim-to-Phishing-Scam.html.

IG Group (2003 – 2019) ¿Qué son las criptomonedas? IG Group. Recuperado de https://www.ig.com/es/invertir-en-criptomonedas/que-son-las-criptomonedas.

Labaca Castro, R. (8 de abril de 2011) Robo de identidad y sus cifras en América Latina. Pagina We Live Security. Recuperado de https://www.welivesecurity.com/la-es/2011/04/08/robo-identidad-cifras-america-latina/.

LexJuris (n/a) Apropiación ilegal. Recuperado de http://www.lexjuris.com/penal/lexpenal5.htm.

Malby, S. (febrero del 2013) Estudio Exhaustivo sobre el delito cibernético. Documento PDF de la Oficina de las Naciones Unidas contra la Droga y el Delito. Recuperado de https://www.unodc.org/documents/organized crime/cybercrime/Cybercrime_Study_Spanish.pdf.

Mikoluk, K. (18 de septiembre de 2013) Xampp Parental Control. Udemy. Recuperado de https://blog.udemy.com/xampp-tutorial/.

National Insitute of Standards and Technology (2006). Guide to Integrating Forensic Techniques

into Incident Response. U.S. Department of Commerce. Recuperado de: https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response.

Oracle (2014) Glosario de términos de redes. Oracle. Recuperado de https://docs.oracle.com/cd/E56339_01/html/E53820/gnchw.html.

Rubén A. (4 de marzo de 2016) *Kali Linux*. Computer Hoy. Recuperado de https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671.

Steer, J. (2016, December 16). 3 *Romanian nationals charged in cyber fraud scheme targeting*. Ohioans FOX 8. Recuperado de https://fox8.com/2016/12/16/three-charged-with-stealing-millions-in-international-cyber-fraud-conspiracy/.

United States Department of Justice (15 de julio de 2015) USA vs Solomon Oyesanya. Recuperado de https://www.justice.gov/usao-edva/pr/brooklyn-man-sentenced-conspiracy-defraud-us-defense-contractors-and-id-theft-fraud.

United States Department of Justice (21 de abril de 2017) USA vs Fabio Gasperini. Recuperado de https://www.justice.gov/usao-edny/pr/cybercriminal-who-created-global-botnet-infected-malicious-software-extradited-face.

United States Department of Justice (16 de febrero de 2017) USA vs Timothy Livingston. Recuperado de https://www.justice.gov/opa/pr/florida-man-sentenced-hacking-spamming-scheme-used-stolen-email-accounts.

United States vs Bogdan Nicolescu, Tiberiu Danes, Radu Miclaus, 1:16-cr0024 (United States Department of Justice 2016).

Wells, J.T. (2013). *Principles of fraud examination* (4th ed.). New Jersey. John Wiley & sons, Inc.

Yong, N. (9 de noviembre de 2018) Detectando fraudes a través del análisis de datos. Pagina Recuperado de https://gestion.pe/blog/brujula-de-gestion-empresarial/2018/09/detectando-fraudes-a-traves-del-analisis-de-datos.html?ref=gesr.