EDP UNIVERSITY OF PUERTO RICO, INC.
RECINTO DE HATO REY
PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACIÒN CON ESPECIALIDAD EN SEGURIDAD DE INFORMACIÒN E INVESTIGACIÒN DE FRAUDE

FRAUDE CIBERNETICO: COMO INFLUYE LA FALTA DE CONTROLES DE SEGURIDAD Y CONOCIMIENTO EN LOS ATAQUES CIBERNETICOS TANTO EN EMPRESAS PRIVADAS Y GUBERNAMENTALES COMO A NIVEL INDIVIDUAL

Análisis de Caso: United_States VS. Zhu Hua and Zhang Shilong

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÒN CON ESPECIALIDAD EN SEGURIDAD DE INFORMACIÒN E INVESTIGACIÒN DE FRAUDE

MARZO/ 2020

PREPARADO POR
DANIEL A. SILVA FIGUEROA

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

FRAUDE CIBERNETICO: COMO INFLUYE LA FALTA DE CONTROLES DE SEGURIDAD Y CONOCIMIENTO EN LOS ATAQUES CIBERNETICOS TANTO EN EMPRESAS PRIVADAS Y GUBERNAMENTALES COMO A NIVEL INDIVIDUAL

Análisis de Caso: United_States VS. Zhu Hua and Zhang Shilong

Preparado por
Daniel A. Silva Figueroa

Ha sido aceptado como requisito parcial para el grado de
Maestría en Sistemas de Información con Especialidad en
Seguridad de Información e Investigación de Fraude (MISFI)

Marzo, 2020

Aprobado por:

Dr. Miguel A. Drouyn Marrero, Profesor

Tabla de Contenido

Lista de Figuras

Sección 1: Introducción y Trasfondo

Introducción

Actualmente los fraudes en los sistemas de información son un gran problema para la sociedad por lo avanzada que se encuentra la tecnología. Ante la extensión y la utilidad que tiene la tecnología en nuestras vidas y la cantidad de personas en el mundo que la utilizan tiene como resultado que también la delincuencia se haya expandido en esa dimensión. Debido al anonimato y a la información personal que se guarda en el Internet, el poder atrapar los delincuentes se convierte cada vez en una tarea más difícil para identificarlos. Esto lo veremos más adelante en el caso 2018_12_20 UNITED STATES V. ZHU HUA and ZHANG SHILONG el cual está relacionado con los casos de fraude en los sistemas informáticos.

Estos casos de fraude en los sistemas informáticos han ido creciendo y se pueden ver reflejados en este caso, en el cual los acusados se encontraban cometiendo delitos cibernéticos desde 2006 y no es hasta 2018 que logran acusarlos. Con la discusión de este caso se busca que todas las entidades, agencias y comunidades a integrar, educar y persuadirlos en el campo de las computadoras e integrar controles y medidas de seguridad en las mismas. Mi interés por la investigación y el combatir los fraudes comenzó desde pequeño ya que mi padre trabaja para la Policía de Puerto Rico y diariamente discutíamos sobre diferentes situaciones del país y de su diario vivir. Me preocupa mucho la situación en cuanto a los fraudes cometidos en este caso ya que más de 12 países fueron víctimas de fraude por parte de este Grupo APT10 junto con los acusados ZHU HUA y ZHANG SHILONG. Algunas de las agencias que se podrían beneficiar del análisis de este caso y su solución lo son el Negociado de la Policía de Puerto Rico, Departamento de Educación y el Departamento de Hacienda que son las agencias más grandes que tiene el

Gobierno de Puerto Rico. Otra entidad que se podría beneficiar del estudio de este caso es EDP University y otras entidades universitarias donde pueden crear programas relacionados a cómo combatir el crimen, como, por ejemplo, la maestría la cual me encuentro cursando que es en Sistemas de Información con especialización en Fraude Digital y Seguridad de la Información.

El poder estudiar y discutir este caso permitirá que las agencias y entidades antes mencionadas puedan identificar sus vulnerabilidades y crear políticas de prevención para mitigar el riesgo. El resolver este caso es importante ya que todas estas agencias y entidades victimas del fraude por parte de los acusados pudieron identificar sus vulnerabilidades y mejorar su seguridad. También la comunidad verificar sus sistemas y reforzarlos.

Descripción del caso:

Número del caso- 2018_12_20_United_States VS. Zhu Hua and Zhang Shilong

Partes en el caso-

Acusado(s)

- ZHU HUA ALIAS “Afwar”, "CVNX”, "Alayos”, "Godkiller,"
- ZHANG SHILONG ALIAS "Baobeilong”, "Zhang Jianguo” "Atreexp,"
- Miembros del Grupo APTlO (Advanced Persistent Threat 10)

Víctimas u otras personas o entidades involucradas-

- Compañía “Huaying Haitai Science and Technology Development” ("Huaying Haitai") en Tianjin, China
- Oficina de Seguridad del Estado de Tianjin del Ministerio de Seguridad del Estado de China.

- 45 entidades con sede en al menos 12 estados, incluidos Arizona, California, Connecticut, Florida, Maryland, Nueva York, Ohio, Pensilvania, Texas, Utah, Virginia y Wisconsin
- Clientes del MSP ubicados en al menos 12 países, incluidos Brasil, Canadá, Finlandia, Francia, Alemania, India, Japón, Suecia, Suiza, los Emiratos Árabes Unidos, el Reino Unido y los Estados Unidos.
- Department of Navy of the United States

Investigadores- FBI, DCIS Y NCIS

Abogados- Matthew Chang- Litigante

Fiscales:

- Geoffrey S. Berman- US Attorney General
- Sagar K. Ravi- Fiscal Federal de la unidad de Fraudes y Ciberdelitos del Estado de Nueva York
- John C. Demers- Assistant Attorney General for National Security

Jueces- Debra C. Freeman, Corte del Distrito Sur de Nueva York de los Estados Unidos

Trasfondo:

Según la acusación en USA vs. ZHU HUA y ZHANG SHILONG (2018), los acusados, quienes eran nacionales de la República Popular de China ("China"), eran miembros de un grupo de piratería que operaba en China, conocido dentro de la comunidad de seguridad cibernética como el "Grupo APTlO"(Advanced Persistent Threat 10). Estos son acusados por desde o alrededor de 2006 hasta alrededor del 2018, por robar tecnologías y otra información de valor para la conspiración. Los acusados trabajaron para la Compañía de Desarrollo de Ciencia y Tecnología

Huaying Haitai ("Huaying Haitai") en Tianjin, China, y actuaron en asociación con la Oficina de Seguridad del Estado de Tianjin del Ministerio de Seguridad del Estado de China. Los miembros del Grupo APTlO trabajaban en un entorno de oficina y generalmente se dedicaban a piratear operaciones durante el horario laboral en China. La denuncia o queja inicial comenzó con la campaña de robo de tecnología para el 2006 donde el APTlO Group robó cientos de gigabytes de datos confidenciales y apuntó a las computadoras de las compañías víctimas involucradas en una amplia gama de actividades comerciales, industrias y tecnologías, que incluyen tecnología de aviación, espacio y satélite, tecnología de fabricación, tecnología farmacéutica, exploración y producción de petróleo y gas tecnología, tecnología de comunicaciones, tecnología de procesador de computadora y tecnología marítima.

El Grupo APTlO, alrededor del 2014, apuntó a los MSP para aprovechar las redes de los MSP para obtener acceso no autorizado a las computadoras y las redes informáticas de los clientes de los MSP y robar propiedad intelectual y datos comerciales confidenciales a escala global, por ejemplo, a través de MSP Theft Campaign. Aquí se vio involucrada información de alrededor 12 países incluidos Brasil, Canadá, Finlandia, Francia, Alemania, India, Japón, Suecia, Suiza, los Emiratos Árabes Unidos, el Reino Unido y los Estados Unidos. La información comprometida incluía compañías que estaban involucradas en una amplia gama de actividades comerciales, industriales y tecnológicas, incluyendo banca y finanzas, telecomunicaciones y electrónica de consumo, equipos médicos, empaques, manufactura, consultoría, atención médica, biotecnología, automotriz, petróleo y gas. exploración y minería.

Descripción de hechos:

Según los documentos del caso USA vs Zhu Hua and Zhang Shilong (2018) a partir de 2006, los miembros del Grupo APTlO, incluidos ZHU HUA y ZHANG SHILONG, los acusados, participaron en una campaña de intrusión donde obtuvieron el acceso no autorizado a las computadoras y redes de computadoras de empresas comerciales, tecnología de defensa y agencias del gobierno de los Estados Unidos para robar información y datos sobre una serie de tecnologías (la "Campaña de robo de tecnología"). A través de la Campaña de robo de tecnología, el APTlO Group robó cientos de gigabytes de datos confidenciales y apuntó a las computadoras de las compañías víctimas donde la información era relacionada a tecnología de aviación, espacio y satélite, tecnología de fabricación, tecnología farmacéutica, exploración y producción de petróleo y gas tecnología, tecnología de comunicaciones, tecnología de procesador de computadora y tecnología marítima. En 2014, este mismo grupo, incluidos ZHU y ZHANG, fueron parte de una campaña de intrusión donde obtuvieron acceso no autorizado a las computadoras y las redes informáticas de los proveedores de servicios administrados ("MSP") para empresas y gobiernos de todo el mundo. Además, el Grupo APTlO comprometió más de 40 computadoras para robar datos confidenciales de los sistemas que pertenecen al Departamento de Marina de los Estados Unidos (la "Marina"), incluida la información de identificación personal de más de 100,000 miembros del personal de la Marina.

Acusaciones, cargos y penalidades:

- **Cargo 1: Title 18, United States Code, Sections 1030 (a)(2)(C), 1030 (c)(2) (B)(iii), 1030 (a)(4), 1030 (c)(3)(A), 1030·(a)(5) (A), 1030 (c) (4)(A) (i)(I) & (VI), and 1030 (c)(4) (B)(i) -** combinaron, conspiraron, confederaron y acordaron juntos y entre sí comprometerse a cometer delitos de intrusión informática.
- **Cargo 2: Title 18, United States Code, Sections 1030 (a)(2)(C), 1030 (c)(2) (B)(iii) –** los acusados lograron acceso intencional a las computadoras sin autorización, y excedieron el acceso autorizado, y de ese modo obtuvieron información de computadoras protegidas, y el valor de la información obtenida excedía los $ 5,000
- **Cargo 3: Title 18, United States Code, Sections 1030 (a)(4) and 1030 (c)(3)(A) -** los acusados y otros conocidos y desconocidos, a sabiendas y con la intención de defraudar, accedieron a computadoras protegidas sin autorización, y excedieron el acceso autorizado, y por medio de tal conducta promovieron el fraude previsto, obteniendo cualquier cosa de valor
- **Cargo 4: Título 18, Código de los Estados Unidos, Secciones 1030 (a) (5) (A), 1030 (c) (4) (A) (i) (I) y (VI), y 1030 (c) (4) (B) (i) -** causaron las transmisiones de programas, información, códigos y comandos, y como resultado de tal conducta, causaron daños intencionalmente sin autorización a las computadoras protegidas, lo que causó la pérdida de una o más personas durante cualquier período de un año al menos de $ 5,000 en valor y daños que afectan a diez o más computadoras protegidas durante un período de un año
- **Cargo 5: Title 18, United States Code, Section 1343 –** conspiraron y acordaron juntos para entre sí cometer fraude electrónico. Participaron en un esquema junto con otros para

obtener de manera fraudulenta propiedad intelectual e información comercial o tecnológica confidencial de las compañías víctimas mediante el acceso remoto a través de Internet y sin autorización, a las computadoras de las víctimas utilizando credenciales de inicio de sesión robadas de los empleados víctimas.

- **Cargo 6: Title 18, United States Code, Section 1349 y 3238** - Los acusados y otros conocidos y desconocidos, con la intención premeditada idearon un esquema para defraudar y obtener el dinero y la propiedad por medio de pretensiones, representaciones y promesas falsas y fraudulentas. Transmitieron y causaron por medio de comunicaciones por cable, radio y televisión en el comercio interestatal y extranjero, escritos, letreros, señales, imágenes y sonidos con el propósito de ejecutar dicho esquema.
- **Cargo 7: Title 18, United States Code, Sections 1028A(a) (1) (b), and (c), 3238 and 2 –** los acusados transfirieron y utilizaron sin autorización legal un medio de identificación de otra persona. Ayudaron a la transferencia, posesión y uso del nombre de otra persona y sus credenciales para iniciar sesiones con su nombre de usuario y contraseñas para cometer fraude informático

Definición de términos:

- **Malware**- Según Avast (s.f.), el malware es cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil. Los hackers utilizan el malware con múltiples finalidades, tales como extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo. Puede protegerse contra el malware mediante el uso de software antimalware.
- **Phising-** El phishing es definido en Avast (s.f.) como un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o

datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

- **Seguridad cibernética** – también definida como seguridad informática es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema. La seguridad informática se caracteriza por la protección de datos y de comunicaciones en una red asegurando, en la medida de lo posible, los tres principios básicos: La integridad de los datos: la modificación de cualquier tipo de información debe ser conocido y autorizado por el autor o entidad, la disponibilidad del sistema: la operación continua para mantener la productividad y la credibilidad de la empresa y la confidencialidad: la divulgación de datos debe ser autorizada y los datos protegidos contra ataques que violen este principio. Esta es una disciplina o rama de la Tecnología de la información, que estudia e implementa las amenazas y vulnerabilidades de los sistemas informáticos especialmente en la red como, por ejemplo, virus, gusanos, caballos de troya, ciber-ataques, ataques de invasión, robo de identidad, robo de datos, adivinación de contraseñas, intercepción de comunicaciones electrónicas, entre otros (Significado de seguridad informática, 2019).
- **MSP (Managed Service Provider)**- un proveedor de servicios gestionados (MSP, por sus siglas en inglés) es una compañía que administra de forma remota la infraestructura de TI y/o los sistemas de usuario final de un cliente, generalmente de forma proactiva y bajo un modelo de suscripción.

- **Piratería -** piratería es una forma moderna de quebrantar la ley, pero usando para ello medios informáticos. Los perjudicados por la piratería son casi todas las personas, instituciones públicas, empresas, fundaciones, etc. que no sean conscientes de su existencia. Para cualquier persona que trabaje con ordenadores conectados a la red de redes o Internet, es obligatorio saber que existe, ya que ignorarla puede significar perder nuestros datos almacenados o bien tener que instalar de nuevo el Sistema Operativo del ordenador, con el consecuente gasto que requiere. Un pirata es una persona que crea mediante sus conocimientos de informática, programas para hacer que otras gentes paguen dinero por protegerse y cuya única finalidad es infiltrarse en el ordenador de la víctima para así extorsionarla, espiarla o en el peor de los casos destruir toda su información (Cano Francisco, 2014).
- **Fraude informático** – El fraude cibernético e informático se refiere al fraude realizado a través del uso de una computadora o del Internet. La piratería informática (hacking) es una forma común de fraude: el delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a una computadora con información confidencial. Otra forma de fraude involucra la intercepción de una transmisión electrónica. Esto puede ocasionar el robo de la contraseña, el número de cuenta de una tarjeta de crédito u otra información confidencial sobre la identidad de una persona. La ley federal define al fraude electrónico como el uso de una computadora con el objetivo de distorsionar datos para inducir a otra persona a que haga o deje de hacer algo que ocasiona una pérdida. Los delincuentes pueden distorsionar los datos de diferentes maneras. Primero, pueden alterar sin autorización los datos ingresados en la computadora. Los empleados pueden usar fácilmente este método para alterar esta información y malversar fondos. En segundo lugar, los delincuentes pueden

alterar o borrar información almacenada. Tercero, los delincuentes sofisticados pueden reescribir los códigos de software y cargarlos en la computadora central de un banco para que éste les suministre las identidades de los usuarios. Los estafadores luego pueden usar esta información para realizar compras no autorizadas con tarjetas de crédito (Fraude cibernético e informático, s.f.).

- **Acceso Remoto** - El acceso remoto es el acto de conectarse a servicios, aplicaciones o datos de TI desde una ubicación distinta a la sede central o una ubicación más cercana al centro de datos. Esta conexión permite a los usuarios acceder a una red o una computadora de forma remota a través de una conexión a Internet o telecomunicaciones. El acceso remoto es perfecto para los teletrabajadores, contratistas, aquellos que trabajan desde casa o individuos desplazados de su oficina debido a desastres naturales u otras circunstancias. Es valioso para los negocios que tienen una estrategia para permitir el acceso remoto a sus usuarios. Los empleados pueden tener la flexibilidad de trabajar desde casa o tener un plan instaurado si no pueden ir a la oficina durante un desastre natural (¿qué es el acceso remoto?, s.f.)

Sección 2: Revisión de literatura

Introducción

Un sistema de información tiene como función crear, almacenar, procesar y distribuir la información. El fraude cibernético e informático es el fraude que es realizado a través del uso de una computadora, dispositivo o a través del Internet. Diariamente nosotros nos encontramos expuestos a ser timados mediante un fraude a través de los sistemas de información. Esto constituye un problema a nivel mundial, el cual ha ido creciendo gracias al avance que tiene la tecnología hoy día.

En el 2019, según Witt se reportaron alrededor de 3 millones de casos a nivel de casos relacionados a fraudes cibernéticos. En el 2020 según Vaca se reportaron a la Federal Trade Commission FTC) más de 3.2 millones de casos de fraude. En 2018 se reportó a la FTC pérdidas de dinero de 1.48 mil millones de dólares debido a los fraudes. Sin embargo, si pensábamos que los fraudes eran cometidos más a personas mayores no es así. El mayor índice de casos lo tuvieron jóvenes de entre 20 y 29 años.

El fraude informático se define en la ley federal de Abuso y Fraude Informático (CFAA, por sus siglas en inglés) como el acceso a una computadora protegida sin autorización o excedente de autorización. Esto puede afectar el comercio o comunicación interestatal o extranjera, incluyendo una computadora ubicada fuera de los Estados Unidos. La Ley de Abuso y Fraude Informático (CFAA) prohíbe el espionaje informático, la intrusión informática en computadoras privadas o públicas, cometer fraude con una computadora, la distribución de código malicioso, el tráfico de contraseñas y amenazar con dañar una computadora protegida. Aunque el CFAA es principalmente un estatuto criminal, define una causa civil de acción en § 1030 (g) (Computer and internet fraud, s.f.).

Los ejemplos de fraude informático o de Internet en acción, según esta ley, incluye: correos electrónicos donde solicitan dinero a cambio de pequeños depósitos, también conocido como una estafa de tarifas anticipadas(inversión), correos electrónicos que intentan recopilar información personal como números de cuenta, números de Seguro Social y contraseñas, también conocido como “phishing”, un ejemplo de este es el caso de PayPal. El usar la computadora de otra persona para acceder a información personal con la intención de usarla de manera fraudulenta, instalar spyware o malware para participar en la minería de datos, violar las leyes de copyright al copiar información con la intención de venderla como lo es por ejemplo acceder a las licencias de programas de Office sin pagar el mismo, hackear o usar ilegalmente una computadora para cambiar información, como calificaciones, informes de trabajo, etc. y enviar virus informáticos o gusanos con la intención de destruir o arruinar la computadora de otro.

La figura 1 muestra los porcientos de ocurrencia de estos delitos

A.46.71% son **Delitos Informáticos** como la falsificación o fraude informático mediante la introducción, borrado o supresión de datos informáticos, o la interferencia en sistemas informáticos.

B. 43.11% son **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos**. Dentro de esta categoría las conductas que más se repiten son con un 63.89% delitos relacionados con el acceso ilícito a sistemas informáticos, y con un 36.11% todas aquellas conductas delictivas relativas a la interferencia en el funcionamiento de un sistema informático.

C. 10.18% son **Delitos relacionados con el contenido,** como la producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o

posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

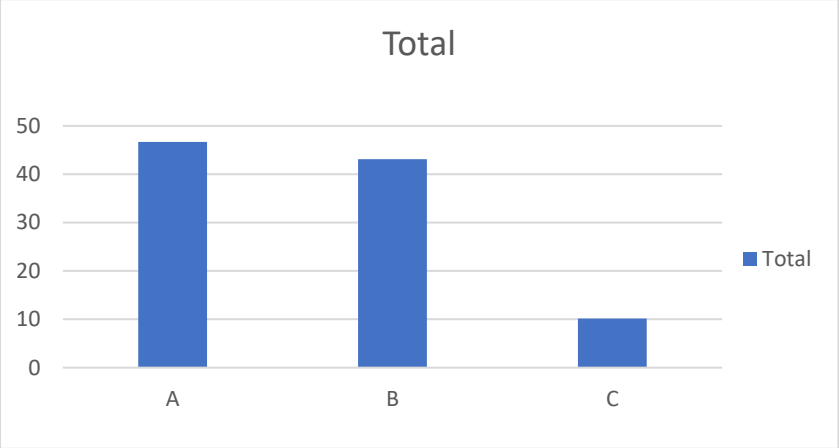


Figura 1: Delitos en la Internet

Según Cobb (2019), estudios relacionados al fraude cibernético muestran que los riesgos de convertirse en víctima de un crimen cibernético son mayores en Estados Unidos. Encuestas realizadas sobre lo que dice la creciente preocupación pública de ser víctima del cibercrimen sobre los esfuerzos de los gobiernos y las empresas por disuadir la ciberdelincuencia nos muestra las siguientes graficas relacionadas a este delito y su aumento.

Figura 2: Riesgo de convertirse en víctima de cibercrimen. Obtenido de Cobb (2019).

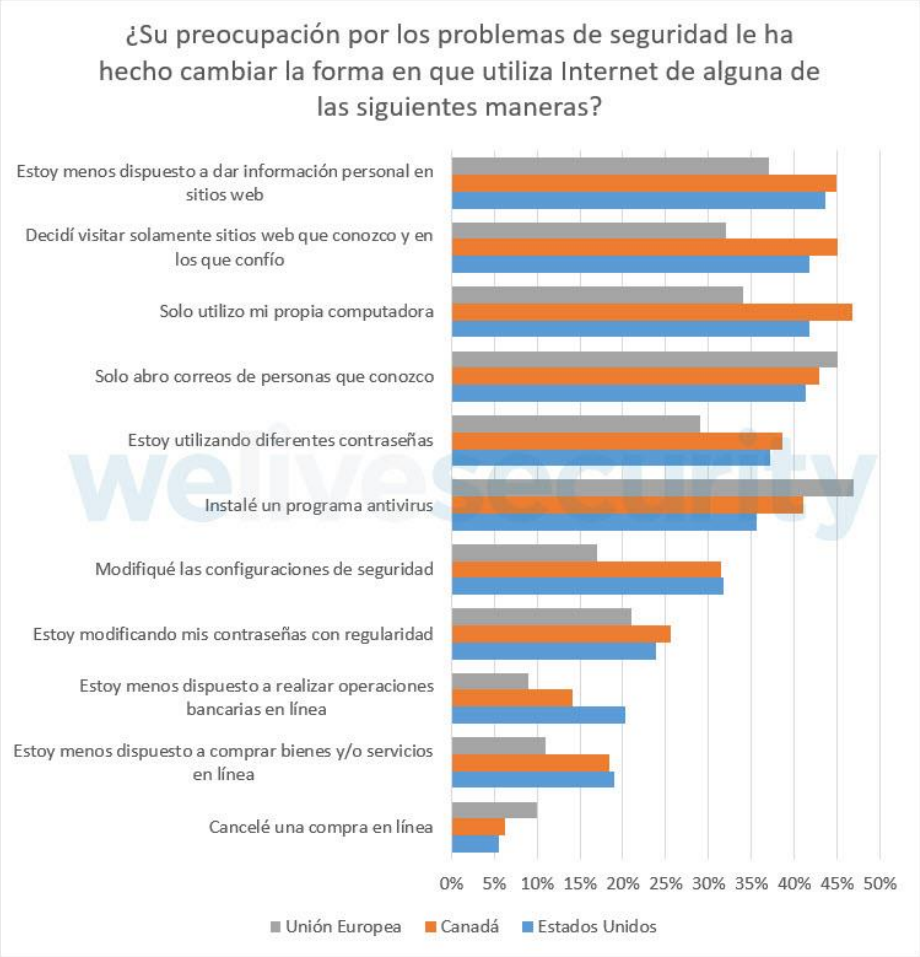


Figura 3: Resultados ante problemas de seguridad, Obtenido de Cobb (2019).

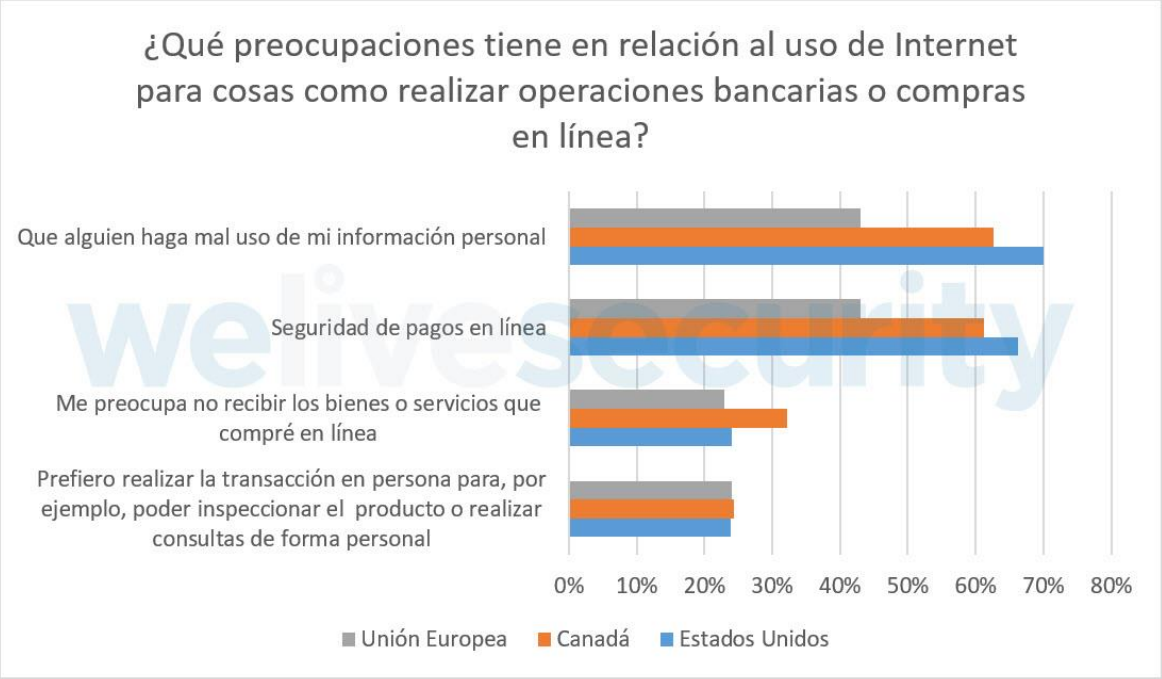


Figura 4: Resultados de países y como utilizan el Internet. Obtenido de Cobb (2019).

Como vemos, Estados Unidos cada día se vuelve más vulnerable y menos seguro para este delito y la desconfianza de las personas es mayor en este continente.

Fraudes Involucrados

- **Robo de información confidencial**

Ethics Global (2016) nos habla del robo de información confidencial definiéndolo como la copia, destrucción, modificación o esconder información confidencial de una persona o empresa. Puede ser desde mapas, correos electrónicos, bases de datos u otro dato susceptible. Este robo puede provocar problemas de competencia desleal, fraude empresarial, espionaje industrial y pérdida de información, llevando en muchos casos hasta la quiebra.

- **Espionaje**

El espionaje es la forma en la que obtenemos información privada de una persona u o empresa, utilizando técnicas basadas en el robo de datos a través de la penetración, infiltración, chantaje o soborno. En el espionaje informático una persona puede acechar, observar a alguien o algo para conseguir información sobre esa persona, empresa o gobierno. Al haber tanto desarrollo y alcance tecnológico, no sólo existe el espionaje entre gobiernos, sino que el espionaje industrial e informático ha cobrado gran fuerza. Entre las herramientas utilizadas para el espionaje informático están: tintas invisibles, micrófonos, grabadoras, micro cámaras, computadoras y los dispositivos móviles que graban video, audio, ubicaciones, y datos (Quanti Solutions, 2018).

- **Acceso a computadoras protegidas**

VIU (2019) se refiere a mantener suficientes controles de seguridad para que ningún intruso pueda acceder los datos de la computadora protegida. Para esto se debe tener seguridad cibernética que es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

- **Fraude a través de cable radio o televisión**

Es el fraude que llamamos de telecomunicaciones donde los delincuentes cuentan con herramientas adecuadas para intervenir tanto en la compañía de telecomunicaciones como en los móviles de los usuarios. Pagar por servicios prestados por terceros sin que el dueño haya

realizado ninguna acción. El primer pago es inmediato, y aunque las cantidades no suelen ser excesivas se repiten sistemáticamente de manera mensual. El ataque implica conseguir el acceso a la cuenta de un usuario de telecomunicaciones legítima para tomar el control de esta según Garatu, G (2019).

Leyes Aplicables

18 U.S.C. 1349 (Intento y conspiración)

De acuerdo con el Código Penal de Estados Unidos, la Sección 1349 del Título 18 se basa en que cualquier persona que intente o conspire para cometer un delito bajo este capítulo, Fraude por Correo y otras ofensas por Fraude será sujeto a las mismas sanciones que las prescritas para el delito, cuya comisión fue objeto del intento o conspiración.

18 U.S.C. 1343 (Fraude electrónico)

De acuerdo al Código Penal de Estados Unidos, la Sección 1343 del Título 18 se basa en que toda persona que haya ideado o tenga la intención de idear algún esquema o artificio para defraudar, o para obtener dinero o propiedad por medio de pretensiones falsas o fraudulentas, representaciones o transmite o hace que se transmita por cable, radio o televisión u otro medio de comunicación en comercio interestatal o extranjero, cualquier escrito, letrero, señal, imágenes o los sonidos con el propósito de ejecutar dicho esquema o artificio, será multado bajo este título o encarcelado no más de 20 años, o ambos. Si la violación ocurre en relación con, o que implique cualquier beneficio autorizado, transportado, transmitido, transferido, desembolsado o pagado en relación con un desastre o emergencia mayor declarado por el presidente de los Estados Unidos, o afecta a una institución financiera, dicha persona será multada no más de $ 1,000,000 o encarcelado no más de 30 años, o ambos.

18 U.S.C. 3238. Delitos no cometidos en ningún distrito

De acuerdo al Código Penal de Estados Unidos, la Sección 3238 del Título 18 se basa en que el juicio de todos los delitos iniciados o cometidos en alta mar, o fuera de la jurisdicción de un Estado o distrito en particular, será en el distrito en el que el delincuente, o cualquier uno de dos o más delincuentes en conjunto, es arrestado o es llevado por primera vez; pero, si dicho delincuente o delincuentes no son arrestados o llevados a ningún distrito, se puede presentar una acusación en el distrito de la última residencia conocida de delincuente, o si no se conoce dicha residencia, la acusación o la información pueden presentarse en el Distrito de Columbia.

18 U.S.C. 1028 Fraude y actividades relacionadas en relación con documentos de identificación, características de autenticación e información

Esta sección proporciona un nivel de penalidades de tres niveles dependiendo de la naturaleza del acto prohibido y el tipo de documento involucrado.

A. La Sección 1028 (b) (1) está dirigida a los productores y traficantes más peligrosos en identificación falsa. Regula los delitos que involucran: (1) la producción o transferencia de un documento de identificación o documento de identificación falso que es o parece ser un documento de identificación de los Estados Unidos o un certificado de nacimiento, licencia de conducir o tarjeta de identificación personal; (2) la producción o transferencia de más de cinco documentos de identificación o documentos de identificación falsos; o (3) la producción, transferencia o posesión de un implemento para hacer documentos bajo la sección 1028 (a) (5).

B. La Sección 1028 (b) (2) crea una penalización intermedia para los otros productores y traficantes si el delito involucra: (1) cualquier producción o transferencia de un documento de identificación o documento de identificación falso que no sea el penalizado por 18 USC § 1028

(b) (1) o (2) la posesión con la intención de usar ilegalmente o transferir ilegalmente cinco o más documentos de identificación (que no sean aquellos emitidos legalmente para el uso del poseedor) o documentos de identificación falsos bajo 18 USC § 1028 (a) (3).

C. La Sección 1028 (b) (3) cubre los delitos menores de 18 USC § 1028 (a) (4) y (a) (6).

Si bien se puede argumentar que la disposición de penalización por un intento no está clara según 18 USC § 1028 (por ejemplo, ¿la palabra "producción" abarca también un intento de producir o es un intento de ser tratado como "cualquier otro caso" bajo 18 USC? § 1028 (b) (3)), el historial legislativo indica de manera concluyente que el Congreso pretendía castigar los intentos al mismo nivel que el delito completo. Los fiscales federales, por lo tanto, deben instar a una pena más alta por intento. Por supuesto, los intentos de violar 18 USC § 1028 (a) (4) y (a) (6) serían delitos menores porque tales delitos son en sí mismos delitos menores.

18 U.S.C. 1030 Fraude y actividades relacionadas en conexión con computadoras

La Ley de Abuso y Fraude Informático (CFAA), 18 U.S.C. 1030, proscribe la conducta que victimiza los sistemas informáticos. Es una ley de seguridad cibernética. Protege las computadoras federales, las computadoras bancarias y las computadoras conectadas a Internet. Esta los protege de intrusos, amenazas, daños, espionaje y de ser utilizados corruptamente como instrumentos de fraude. No es una disposición integral, sino que llena las grietas y lagunas en la protección que brindan otras leyes penales federales. En su forma actual, los siete párrafos de la subsección 1030 (a) proscriben:

• intrusión informática (por ejemplo, piratería informática) en una computadora del gobierno, 18 U.S.C. 1030 (a) (3);

• intrusión informática (por ejemplo, piratería informática) que da como resultado la exposición a cierta información gubernamental, crediticia, financiera o almacenada en la computadora, 18 U.S.C. 1030 (a) (2);

• Dañar una computadora del gobierno, una computadora del banco o una computadora utilizada en el comercio interestatal o extranjero (por ejemplo, un gusano, virus informático, caballo de Troya, bomba de tiempo, un ataque de denegación de servicio y otras formas de ataque cibernético)., delito cibernético o terrorismo cibernético), 18 USC 1030 (a) (5);

• cometer fraude, una parte integral de la cual implica el acceso no autorizado a una computadora del gobierno, una computadora del banco o una computadora utilizada en, o que afecta, el comercio interestatal o extranjero, 18 U.S.C. 1030 (a) (4);

• amenazar con dañar una computadora del gobierno, una computadora del banco o una computadora utilizada en, o que afecte, el comercio interestatal o extranjero, 18 U.S.C. 1030 (a) (7);

• tráfico de contraseñas para una computadora del gobierno, o cuando el tráfico afecta el comercio interestatal o extranjero, 18 U.S.C. 1030 (a) (6); y

• Acceder a una computadora para cometer espionaje, 18 U.S.C. 1030 (a) (1).

La subsección 1030 (b) establece que es un delito intentar o conspirar para cometer cualquiera de estos delitos. La subsección 1030 (c) cataloga las penas por cometerlas, penas que van desde el encarcelamiento por no más de un año por traspaso simple en el ciberespacio hasta un máximo de cadena perpetua cuando la muerte resulta de daños informáticos intencionales. La subsección 1030 (d) conserva la autoridad investigadora del Servicio Secreto. La subsección 1030 (e) proporciona definiciones comunes. La subsección 1030 (f) niega cualquier aplicación a

actividades de aplicación de la ley que de otra manera serían permitidas. La subsección 1030 (g) crea una causa de acción civil para las víctimas de estos crímenes. Las subsecciones 1030 (i) y (j) autorizan la confiscación de bienes contaminados.

Casos relacionados

USA vs. Piotr Levashov (2018)

Un caso relacionado a lo que se está cubriendo en la actualidad es el del pirata informático ruso Piotr Levashov. El ruso enviaba correos basura para dañar equipos informáticos e infectarlos con un programa malicioso llamado "ransomware", que sirve a estos a tomar control del sistema operativo infectado y pedir dinero a sus usuarios a cambio de liberarlo. Utilizaba una "botnet" la cual es una red de computadoras infectadas con un malware que permite controlar todas las computadoras sin el consentimiento de los propietarios. Este recolectaba información personal de las víctimas. Este utilizaba los usuarios, correos para cometer fraude y enriquecerse. Fue arrestado el 7 de abril de 2017.

USA vs. PARK JIN HYOK, also known as ("aka") "Jin Hyok Park," aka "Pak Jin Hek,"(2018)

Otro caso relacionado al del estudio de caso fue el ataque con un ransomware conocido como WannaCry, el cual infectó a unas 300.000 computadoras en 150 países en mayo de 2017. El ransomware es un programa malicioso que ingresa al sistema, encripta archivos y luego pide un dinero de rescate para devolver al usuario la posibilidad de acceder otra vez a ellos. El software cifró los archivos y exigió a los usuarios entregar cientos de dólares a cambio de claves para descifrar los archivos. WannaCry comenzó un 12 de mayo e hizo daño a más de 230 mil computadoras. Los países más perjudicados fueron Rusia; Ucrania; India; Gran Bretaña, donde

se vio comprometido el servicio nacional de salud; España, por el ataque a Telefónica y Alemania, donde la empresa ferroviaria alemana Deutsche Bahn AG fue el principal blanco. El ataque afectó a hospitales, incluidos muchos pertenecientes al Servicio Nacional de Salud (NHS) del Reino Unido, bancos y otras empresas. La compañía FedEx dijo que había perdido cientos de millones de dólares como resultado del ataque. Estados Unidos y Reino Unido culparon a Corea del Norte, una acusación que Pyongyang negó y que calificó de "grave provocación política".

USA vs. Paige A. Thompson (2019)

En este caso Thompson, ingeniera de software de la compañía de Seattle por intrusión no autorizada en datos almacenados de más de 30 compañías diferentes. Se le acusa de fraude electrónico, fraude informático y abuso. Thompson creo un software donde identificaba a los clientes de las empresas victimas que no contenían un buen firewall y poder entrar a sus servidores. La policía se dio cuenta de la actividad de Thompson después de que ella compartió información con otro usuario en la herramienta GitHub en relación con su robo de información de los servidores que almacenan datos de Capital One. El 17 de julio de 2019, el usuario de GitHub alertó a Capital One sobre la posibilidad de que hubiera sufrido un robo de datos. Después de determinar el 19 de julio de 2019 que hubo una intrusión en sus datos, Capital One contactó al FBI (DOJ, 2019).

Herramientas de Investigación

Bulk Extractor

Bulk Extractor es una herramienta forense la cual se caracteriza por su rapidez y capacidad de investigar detalladamente. También detecta, descomprime y analiza utilizando una variedad de algoritmos. Los resultados pueden ser fácilmente inspeccionados, analizados o procesados con

herramientas automatizadas. El programa puede utilizarse para aplicaciones de aplicación de la ley, defensa, inteligencia y ciber investigación (Bulk-extractor, s.f.).

IDEA

IDEA es una poderosa herramienta para análisis, extracción y auditorías basadas en datos, fácil de utilizar (amigable) y provista de numerosas funciones para verificar la calidad e integridad de la información de bases de datos y archivos de computador, identificación y análisis de fraudes.

- Analizar y clasificar los datos aplicando criterios de acuerdo con las reglas del negocio.
- Automatizar técnicas de auditoría asistidas con el computador (CAATs).
- Generación de reportes y gráficos.
- Exportar archivos y enviar correos electrónicos desde el software IDEA.

IDEA ofrece funcionalidades para importar datos de archivos de computador de diferentes formatos (texto, CVS, ODBC, Excel, PDF, reportes, AS400, SAP) e ilimitado número de registros, generar estadísticas de campos numéricos, fecha y hora; realizar operaciones aritméticas, comprobar cálculos, utilizar funciones pre construidas de análisis financiero y manejo de campos, extraer y agrupar registros según criterios especificados por el usuario, identificar registros repetidos y omisiones de secuencia de registros, comparar, unir y agregar archivos, utilizar cinco tipos de muestreo estadístico, identificar operaciones sospechosas de fraude y lavado de activos según (GUIA SOLUCIONES TIC, s.f.).

Metasploit

En conjunto con Rapid7 y la comunidad que colabora con este grupo de código abierto facilita el estar adelantado a cualquier ataque ya que con esa herramienta se puede conocer

vulnerabilidades de seguridad como puertos abiertos y mediante los códigos que debemos reforzar en nuestro sistema informático (Rizaldos, 2018).

Nessus

En la sencillez de Nessus se encuentra uno de los principales incentivos de su disponibilidad por ser un sistema tan simple. Con este programa de escaneo podemos realizar un análisis completo en diversos sistemas donde empieza realizando el escaneo en los puertos y consigue que se puedan detectar todas las vulnerabilidades del entorno informático y así evitar sustos y cualquier tipo de infección (NESSUS, s.f.).

Sección 3: Simulación del Caso

Introducción

Los fraudes cometidos por Zhu Hua y Zhang Shilong junto con el Grupo AP10 en contra de Estados Unidos y otros países fueron perpetrados de una manera inteligente ya que tardaron 12 años en poder encontrar las mentes maestras detrás de estos ataques informáticos. Los acusados formaron parte de intrusiones informáticas a nivel mundial. Estos, junto con el Grupo AP10 desde el 2006 hasta el 2018 utilizaban técnicas para explotar vulnerabilidades en las victimas con el objetivo de robar ya sea propiedad intelectual, información comercial o tecnológica confidencial. El Grupo AP10 comenzó robando información de cientos de gigabytes de datos sobre tecnología confidencial de más de 45 entidades ubicadas en al menos 12 estados.

Utilizaron el método de “spear fishing” para introducir el malware mediante un correo electrónico, donde utilizaron proveedores de servicios del sistema con sus nombres de dominio donde al abrir archivos se instalaba el malware. El malware generalmente incluía variantes personalizadas de un troyano de acceso remoto ("RAT"), incluido uno conocido como "Hiedra Venenosa" y registradores de pulsaciones de teclas, que son programas que registran subrepticiamente. Este se programaba para comunicarse automáticamente con dominios a los que se asignaron direcciones IP de computadoras bajo el control de los miembros del Grupo APTlO, lo que les permite mantener la visibilidad y persistencia acceso remoto a las computadoras comprometidas a través de Internet. después de que el malware se instaló con éxito, el Grupo APTlO descargó malware adicional y herramientas para sistemas informáticos comprometidos con el fin de comprometer aún más las computadoras de la víctima. Después de que el Grupo APTlO obtuvo acceso no autorizado a las computadoras de una víctima e identificó datos de interés en esas computadoras, el Grupo APTlO recopiló los archivos relevantes y otra

información de las computadoras comprometidas y extrajo los archivos e información robados en archivos encriptados a las computadoras bajo su control. De esas entidades se encontraban siete empresas involucradas en tecnología de aviación, espacio y / o satélite, tres empresas involucradas en tecnología de comunicaciones, tres empresas involucradas en la fabricación de sistemas electrónicos avanzados y / o instrumentos analíticos de laboratorio, una empresa involucrada en tecnología marítima, una empresa dedicada a la perforación, producción y procesamiento de petróleo y gas y la NASA.

APTlO Group instaló múltiples variantes personalizadas de malware comúnmente conocidas como PlugX, RedLeaves y QuasarRAT en computadoras MSP ubicadas en todo el mundo. En 2014, en la campaña de robo al MSP el malware que utilizaron para cometer el delito permitió a los miembros del Grupo APTlO monitorear las computadoras de las víctimas de forma remota y robar credenciales de usuario utilizando diversas herramientas de robo de credenciales. En total, el Grupo APTlO registró aproximadamente 1.300 dominios maliciosos únicos en relación con la Campaña contra el robo de MSP. El Grupo APTlO generalmente eliminó los archivos robados de las computadoras comprometidas, buscando así evitar la detección y evitar la identificación de los archivos específicos que fueron robados. Los acusados, obtuvieron con éxito acceso no autorizado a las computadoras que prestan servicios o perteneciente a empresas víctimas ubicadas en al menos 12 países, incluidas al menos las siguientes víctimas:

a. una institución financiera global;

b. tres empresas de telecomunicaciones y / o electrónica de consumo;

c. tres empresas dedicadas a la fabricación comercial o industrial;

d. dos empresas consultoras;

e. una empresa de salud;

f. una empresa de biotecnología;

g. una empresa minera;

h. una empresa proveedora de automóviles; y

i. Una empresa de perforación.

Luego de estos ataques informáticos el Gobierno de EE. UU y empresas privadas como InfraGard publican informes públicos identificando malware y dominios del Grupo AP10, donde luego de esto, los mismos dejaron de usar estos dominios. Finalmente, comprometieron sobre más de 100,000 datos sensitivos del Navy.

Simulación

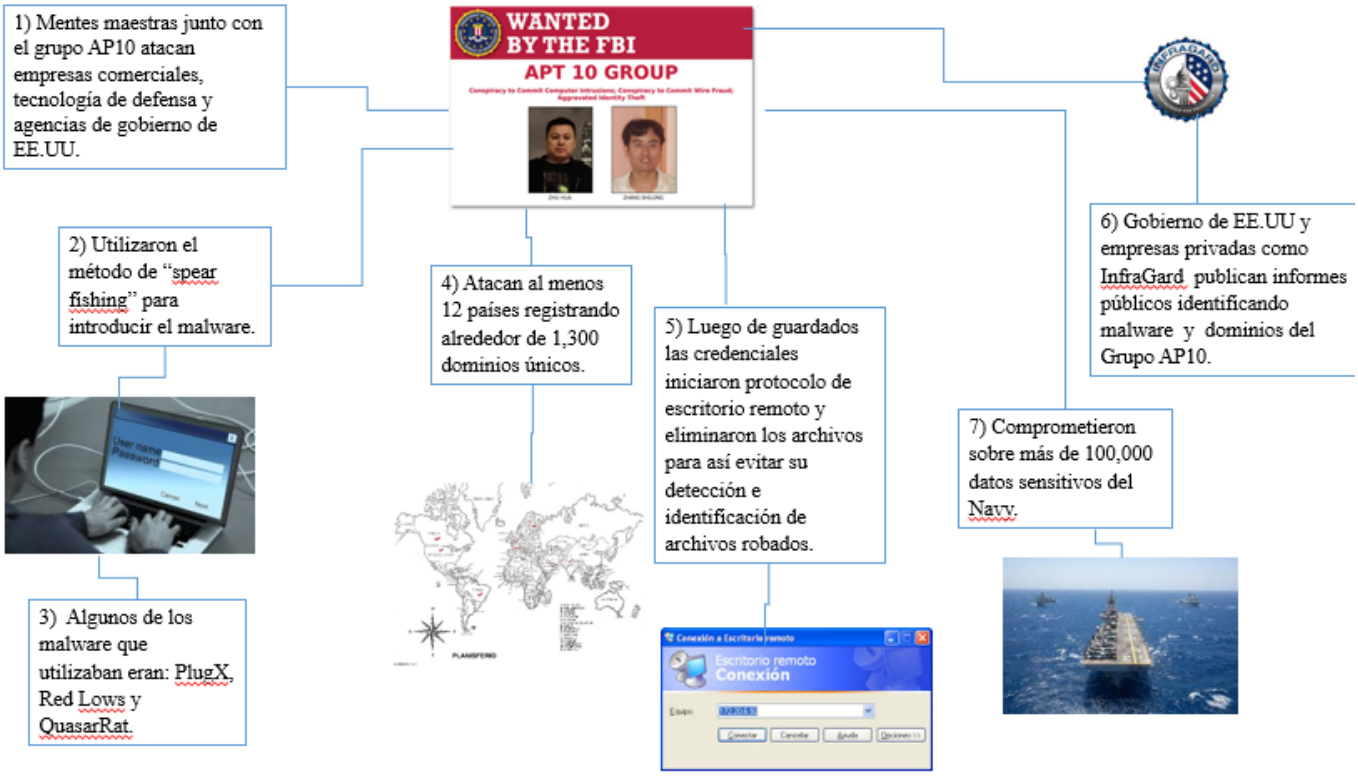


Figura 5: Robo de información confidencial mediante ataque a computadoras protegidas

Sección 4: Informe Forense del Caso

Resumen Ejecutivo

El Departamento de Justicia de Estados Unidos acusa a Zhu Hua y Zhang Shilong de integrar un equipo de hackers que robaron los datos de por lo menos 45 compañías y organizaciones gubernamentales, que incluye el Navy y el robo al MSP Theft Campaign. Estos ciudadanos de la República Popular de China conspiraban para cometer intrusiones informáticas, fraudes electrónicos y robo de identidad. Para el análisis de esta investigación se asignó al agente Daniel A. Silva, experto en fraude cibernético. En esta se analizó una copia del disco duro de los acusados brindada en un USB Lexar 16gb. El mismo fue brindado a Daniel A. Silva por los investigadores del caso, los cuales son el Fiscal Federal Sagar K. Ravi, de la unidad de Fraudes y Ciberdelitos del Estado de Nueva York, junto con el departamento del FBI, DCIS Y NCIS.

De acuerdo con la evidencia obtenida en la investigación, el Sr. Silva indicó que existe relación entre los correos electrónicos encontrados y los archivos que fueron robados por parte de los acusados. Se desconoce el móvil del porqué los acusados tenían información clasificada como nombre, seguro social, salarios, teléfonos, emails, entre otros de las Fuerzas Armadas de la Marina. También se evaluaron los correos electrónicos enviados a las empresas de salud y automóvil, las cuales fueron MedStar Washington Hospital en Washington DC y Copart, los cuales, luego de evaluados, contenían malware. Este malware, el cual se instalaba al abrir el archivo comprimido del correo, está vinculado a los correos enviados por parte de los acusados de los cuales se le imputan.

Objetivo

Para este caso se asignó al agente Daniel A. Silva, donde se analizará una copia del disco duro de la computadora de los acusados Zhu Hua y Zhang Shilong la cual esta copiada a un USB marca Lexar 16gb. La copia del disco duro, provista por los investigadores se examinará utilizando la herramienta FTK Imager para realizar una búsqueda de archivos más a fondo que se relacionen con los delitos que se les imputan a los acusados.

Alcance del trabajo

El 20 de enero de 2019 a las 10:00am en el Tribunal de Nueva York, el Fiscal Federal Sagar K. Ravi, de la unidad de Fraudes y Ciberdelitos del Estado de Nueva York, junto con el departamento del FBI, DCIS Y NCIS hicieron entrega de la copia del disco duro de los acusados en un USB marca Lexar de 16gb al investigador forense Daniel A. Silva. Se recibió junto con la orden, una copia fiel y exacta de los datos. El investigador forense Daniel A. Silva, utilizara la computadora marca HP modelo Notebook la cual contiene los programas FTK Imager e IDEA para analizar la base de datos del MSP y de los archivos que contiene la copia del disco duro en el USB, para asi verificar si existe un vínculo con los acusados. IDEA es una herramienta prestigiosa de auditoria, la cual es utilizada para monitorear bases de datos y procesos para evitar el fraude. La misma genera varios tipos de reportes de la data revisada junto con graficas que ayudan a entender su informe. La otra herramienta FTK ayuda a acceder a archivos e imágenes borrados de la computadora en análisis. Es utilizada frecuentemente en las investigaciones debido a su velocidad, estabilidad y su fácil manejo. Además, esta ayuda a localizar evidencia y a analizar dispositivos digitales como un USB, que almacenan datos.

Datos del Caso

Número del Caso: 2018_12_20 United States vs. Zhu Hua y Zhang Shilong

Investigador: Daniel A. Silva

Cliente solicitante de la Investigación: Departamento de Justicia de Estados Unidos

Representante del Cliente: John C. Demers - Fiscal General Adjunto de Seguridad Nacional

Descripción de los dispositivos utilizados

Durante el proceso de la investigación forense digital se utilizaron los siguientes dispositivos:

1) Computadora portátil marca Hewlett Packard (HP), modelo Notebook, con procesador AMD A8-7410 APU con AMD Readeon R5 Graphics, un disco duro de 900 gb y 8 gb de RAM. La misma cuenta con las herramientas FTK Imager, CaseWare IDEA y otros programas de investigación forense (Figura 6).

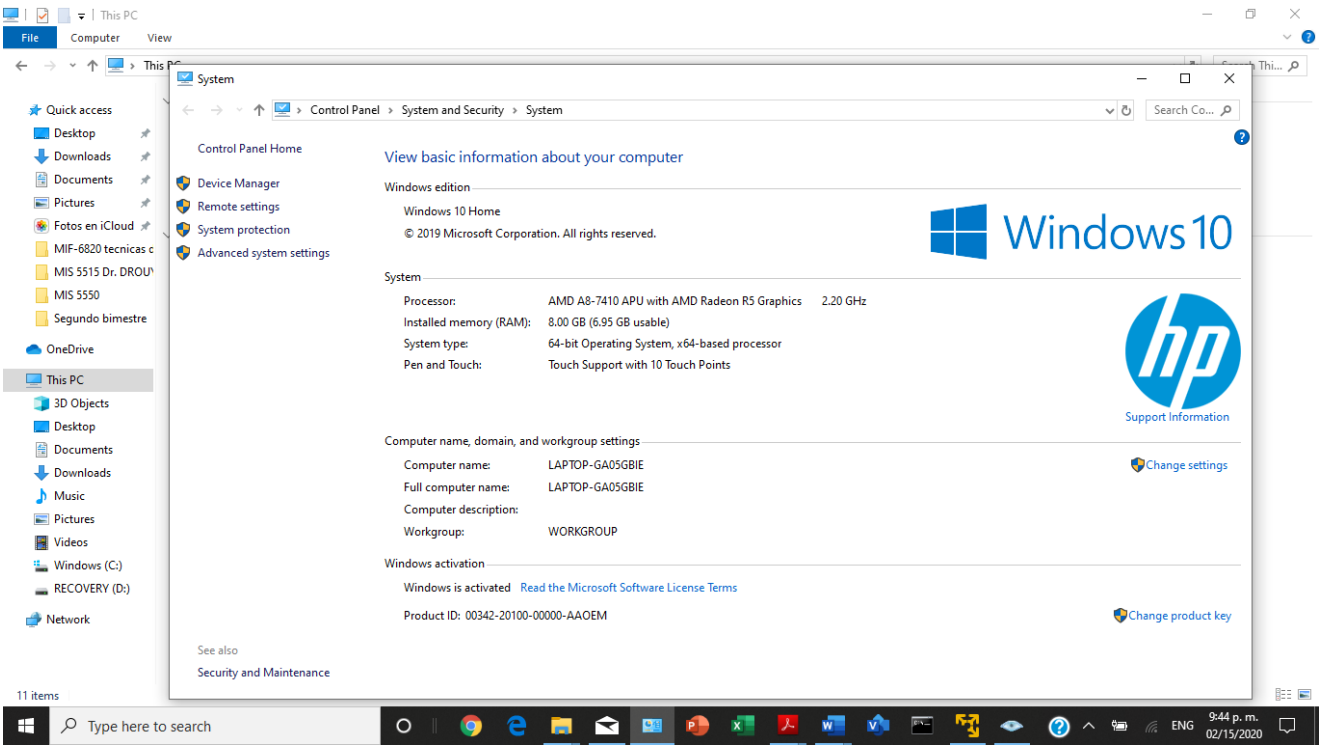


Figura 6: Especificaciones de la computadora HP Notebook utilizada para la investigación

2) USB Drive marca Lexar 16gb que contiene una imagen del disco duro obtenido de los acusados por parte de los investigadores el Fiscal Federal Sagar K. Ravi, de la unidad de Fraudes y Ciberdelitos del Estado de Nueva York, junto con el departamento del FBI, DCIS Y NCIS. Este fue identificado como E2-2018-12-20 (Figura 7).

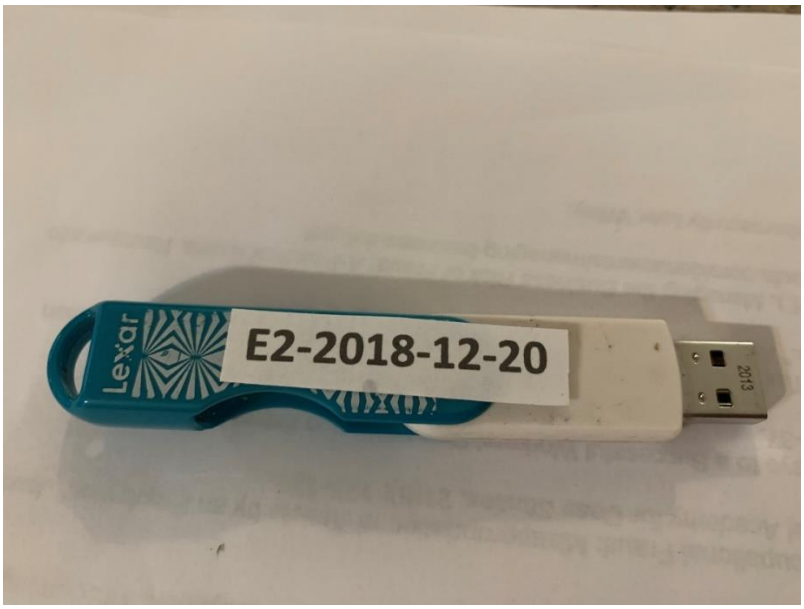


Figura 7: USB con archivos para verificar evidencia

Resumen de Hallazgos

En este resumen vamos a estar identificando los hallazgos obtenidos durante la investigación y análisis de evidencia. Como parte del proceso se utilizaron las herramientas FTK Imager y CaseWare IDEA.

1) En la Figura 8 se muestra un email de una conversación entre el acusado y el grupo AP10 donde le notifica que dicho mensaje tiene un documento anejado para vender información. Estos mencionan que tendrán una conversación por Skype a las 7pm y que todos deben estar presentes. El archivo no está anejado en este email.

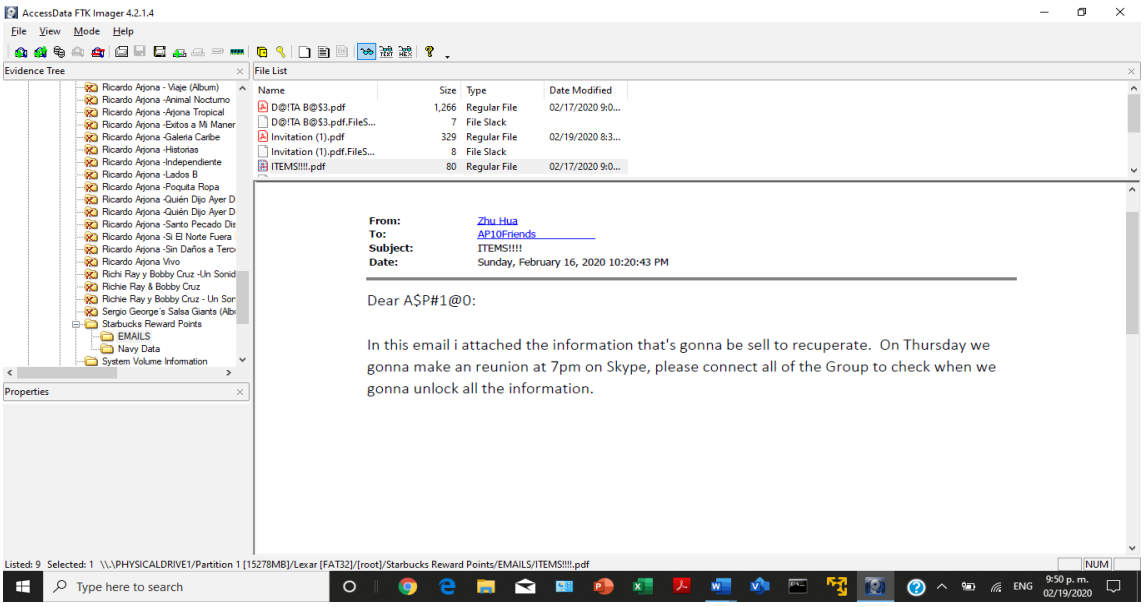


Figura 8: Imagen del correo electrónico entre Zhua Hua y grupo AP10

2) En la Figura 9 se visualiza un archivo .pdf que contiene un correo electrónico entre el acusado Zhu Hua y el grupo AP10 donde el acusado envía como anejo el archivo Excel con los datos antes mencionados y que fue enviado luego del correo electrónico antes mencionado. Este documento presenta evidencia de datos posiblemente robados de las Fuerzas Armadas. Se realizó una extracción de este para así poder ser visto.

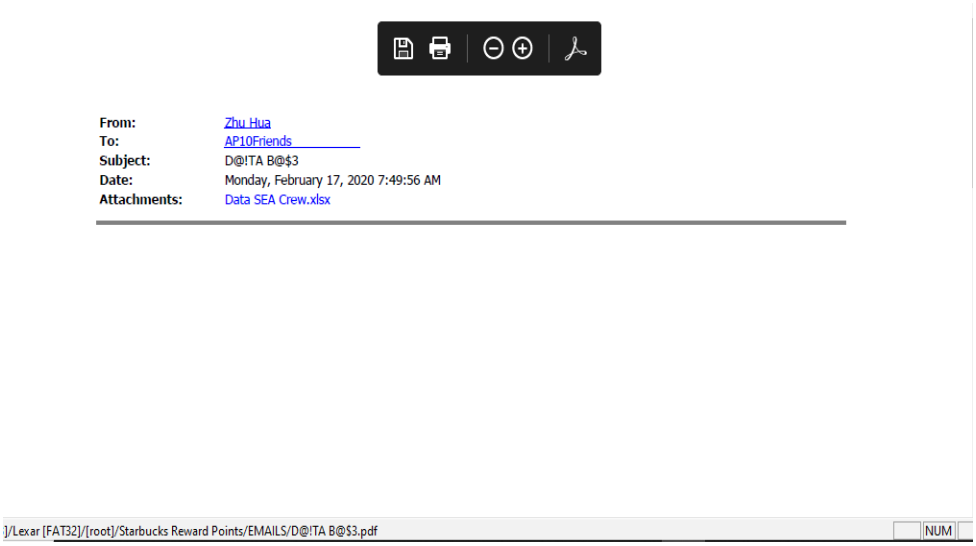
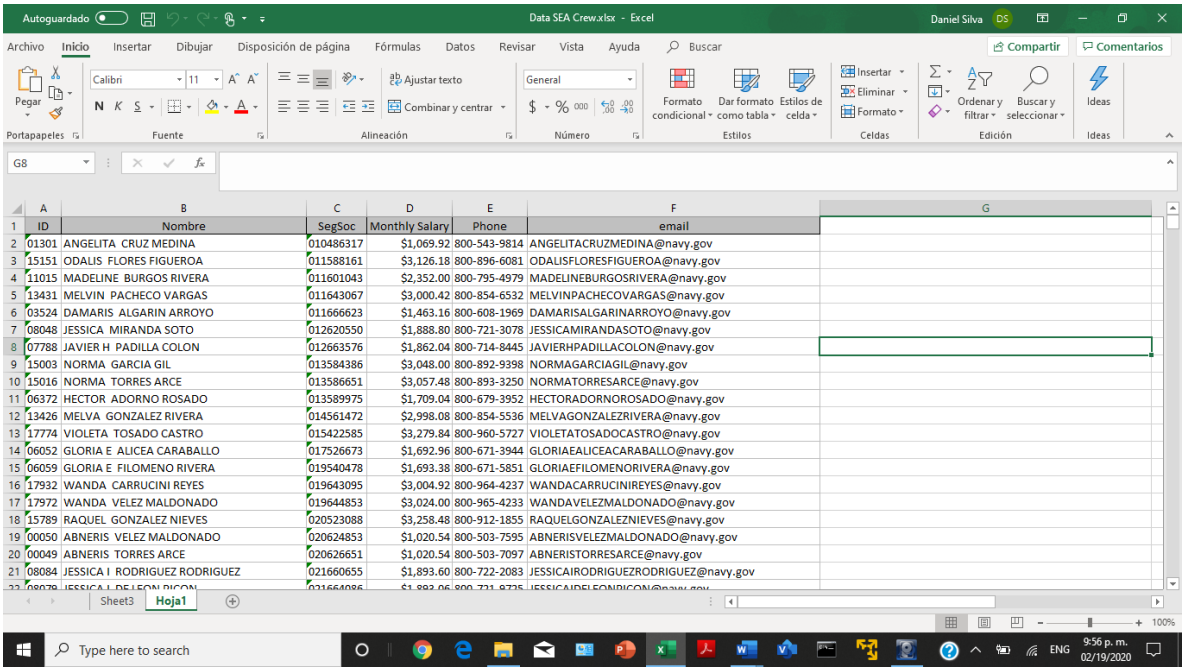


Figura 9: Correo electrónico con archivo Excel

En la Figura 10 se muestra el archivo Excel Data SEA Crew.xls donde se pueden visualizar seis columnas con datos confidenciales que se entiende es la información que fue robada a las Fuerzas Armadas de la Marina.



ID	Nombre	SegSoc	Monthly Salary	Phone	email
01301	ANGELITA CRUZ MEDINA	010486317	$1,069.92	800-543-9814	ANGELITACRUZMEDINA@navy.gov
15151	ODALIS FLORES FIGUEROA	011588161	$3,126.18	800-896-6081	ODALISFLORESFIGUEROA@navy.gov
11015	MADELINE BURGOS RIVERA	011601043	$2,352.00	800-795-4979	MADELINEBURGOSRIVERA@navy.gov
13431	MELVIN PACHECO VARGAS	011643067	$3,000.42	800-854-6532	MELVINPACHECOVARGAS@navy.gov
03524	DAMARIS ALGARIN ARROYO	011666623	$1,463.16	800-608-1969	DAMARISALGARINARROYO@navy.gov
08048	JESSICA MIRANDA SOTO	012620550	$1,888.80	800-721-3078	JESSICAMIRANDASOTO@navy.gov
07788	JAVIER H PADILLA COLON	012663576	$1,862.04	800-714-8445	JAVIERHPADILLACOLON@navy.gov
15003	NORMA GARCIA GIL	013584386	$3,048.00	800-892-9398	NORMAGARCIAGIL@navy.gov
15016	NORMA TORRES ARCE	013586651	$3,057.48	800-893-3250	NORMATORRESARCE@navy.gov
06372	HECTOR ADORNO ROSADO	013589975	$1,709.04	800-679-3952	HECTORADORNOROSADO@navy.gov
13426	MELVA GONZALEZ RIVERA	014561472	$2,998.08	800-854-5536	MELVAGONZALEZRIVERA@navy.gov
17774	VIOLETA TOSADO CASTRO	015422585	$3,279.84	800-960-5727	VIOLETATOSADOCASTRO@navy.gov
06052	GLORIA E ALICEA CARABALLO	017526673	$1,692.96	800-671-3944	GLORIAEALICEACARABALLO@navy.gov
06059	GLORIA E FILOMENO RIVERA	019540478	$1,693.38	800-671-5851	GLORIAEFILOMENORIVERA@navy.gov
17932	WANDA CARRUCINI REYES	019643095	$3,004.92	800-964-4237	WANDACARRUCINIREYES@navy.gov
17972	WANDA VELEZ MALDONADO	019644853	$3,024.00	800-965-4233	WANDAVELEZMALDONADO@navy.gov
15789	RAQUEL GONZALEZ NIEVES	020523088	$3,258.48	800-912-1855	RAQUELGONZALEZNIEVES@navy.gov
00050	ABNERIS VELEZ MALDONADO	020624853	$1,020.54	800-503-7595	ABNERISVELEZMALDONADO@navy.gov
00049	ABNERIS TORRES ARCE	020626651	$1,020.54	800-503-7097	ABNERISTORRESARCE@navy.gov
08084	JESSICA I RODRIGUEZ RODRIGUEZ	021660655	$1,893.60	800-722-2083	JESSICAIRODRIGUEZRODRIGUEZ@navy.gov

Figura 10: Archivo Excel

3) Utilizando la herramienta CaseWare IDEA se pudo comparar el archivo en Excel Data SEA Crew.xls con los datos de las Fuerzas Armadas de la base de datos provista por los investigadores. En esta base de datos la Marina desglosó todos los datos para así identificar las víctimas de este caso (Figura 11). Con el análisis comparativo del archivo Excel y la base de datos se pudo encontrar que efectivamente los datos del archivo Excel eran exactamente los datos de la base, asumiendo así que no hubo pérdida de información. En la Figura 12 se visualiza el resultado utilizando la función JOIN de IDEA para unir ambas bases a través del campo de email y encontrar los datos comunes de ambas. Luego de realizado el "*JOIN"* de ambas tablas se concluyó que no existía perdida de información de la data que fue comprometida a de las Fuerzas Armadas de la Marina.

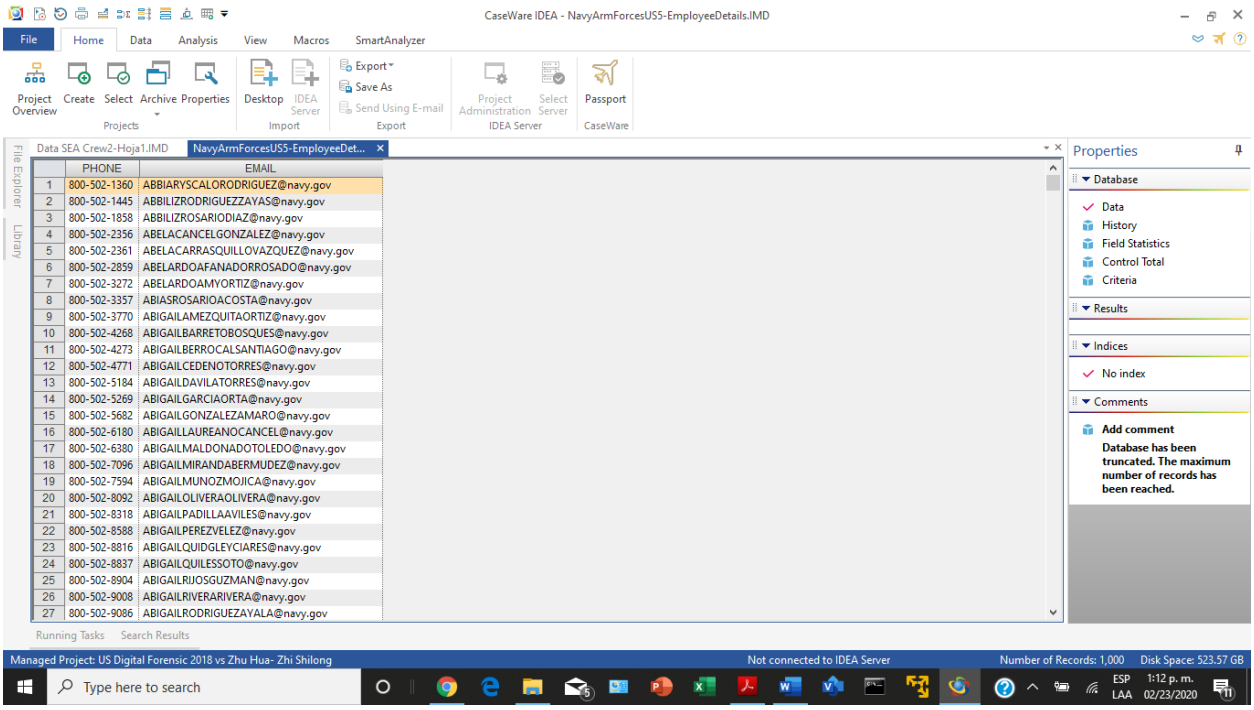
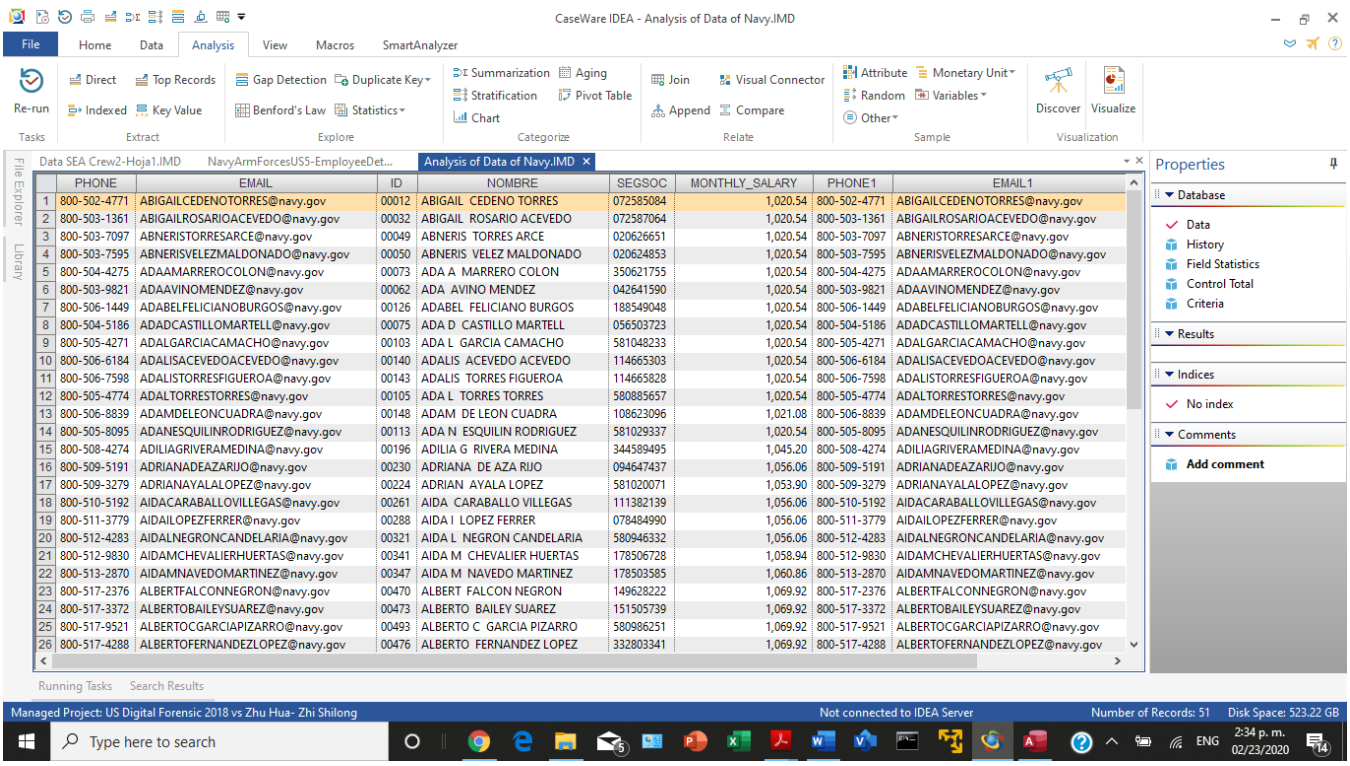


Figura 11: Base provista por las Fuerzas Armadas de la Marina



	PHONE	EMAIL	ID	NOMBRE	SEGSOC	MONTHLY_SALARY	PHONE1	EMAIL1
1	800-502-4771	ABIGAILCEDENOTORRES@navy.gov	00012	ABIGAIL CEDENO TORRES	072585084	1,020.54	800-502-4771	ABIGAILCEDENOTORRES@navy.gov
2	800-503-1361	ABIGAILROSARIOACEVEDO@navy.gov	00032	ABIGAIL ROSARIO ACEVEDO	072587064	1,020.54	800-503-1361	ABIGAILROSARIOACEVEDO@navy.gov
3	800-503-7097	ABNERISTORRESARCE@navy.gov	00049	ABNERIS TORRES ARCE	020626651	1,020.54	800-503-7097	ABNERISTORRESARCE@navy.gov
4	800-503-7595	ABNERISVELEZMALDONADO@navy.gov	00050	ABNERIS VELEZ MALDONADO	020624853	1,020.54	800-503-7595	ABNERISVELEZMALDONADO@navy.gov
5	800-504-4275	ADAAMARREROCOLON@navy.gov	00073	ADA A MARRERO COLON	350621755	1,020.54	800-504-4275	ADAAMARREROCOLON@navy.gov
6	800-503-9821	ADAAVINOMENDEZ@navy.gov	00062	ADA AVINO MENDEZ	042641590	1,020.54	800-503-9821	ADAAVINOMENDEZ@navy.gov
7	800-506-1449	ADABELFELICIANOBURGOS@navy.gov	00126	ADABEL FELICIANO BURGOS	188549048	1,020.54	800-506-1449	ADABELFELICIANOBURGOS@navy.gov
8	800-504-5186	ADADCASTILLOMARTELL@navy.gov	00075	ADA D CASTILLO MARTELL	056503723	1,020.54	800-504-5186	ADADCASTILLOMARTELL@navy.gov
9	800-505-4271	ADALGARCIACAMACHO@navy.gov	00103	ADA L GARCIA CAMACHO	581048233	1,020.54	800-505-4271	ADALGARCIACAMACHO@navy.gov
10	800-506-6184	ADALISACEVEDOACEVEDO@navy.gov	00140	ADALIS ACEVEDO ACEVEDO	114665303	1,020.54	800-506-6184	ADALISACEVEDOACEVEDO@navy.gov
11	800-506-7598	ADALISTORRESFIGUEROA@navy.gov	00143	ADALIS TORRES FIGUEROA	114665828	1,020.54	800-506-7598	ADALISTORRESFIGUEROA@navy.gov
12	800-505-4774	ADALTORRESTORRES@navy.gov	00105	ADA L TORRES TORRES	580885657	1,020.54	800-505-4774	ADALTORRESTORRES@navy.gov
13	800-506-8839	ADAMDELEONCUADRA@navy.gov	00148	ADAM DE LEON CUADRA	108623096	1,021.08	800-506-8839	ADAMDELEONCUADRA@navy.gov
14	800-505-8095	ADANESQUILINRODRIGUEZ@navy.gov	00113	ADA N ESQUILIN RODRIGUEZ	581029337	1,020.54	800-505-8095	ADANESQUILINRODRIGUEZ@navy.gov
15	800-508-4274	ADILIAGRIVERAMEDINA@navy.gov	00196	ADILIA G RIVERA MEDINA	344589495	1,045.20	800-508-4274	ADILIAGRIVERAMEDINA@navy.gov
16	800-509-5191	ADRIANADEAZARIJO@navy.gov	00230	ADRIANA DE AZA RIJO	094647437	1,056.06	800-509-5191	ADRIANADEAZARIJO@navy.gov
17	800-509-3279	ADRIANAYALALOPEZ@navy.gov	00224	ADRIAN AYALA LOPEZ	581020071	1,053.90	800-509-3279	ADRIANAYALALOPEZ@navy.gov
18	800-510-5192	AIDACARABALLOVILLEGAS@navy.gov	00261	AIDA CARABALLO VILLEGAS	111382139	1,056.06	800-510-5192	AIDACARABALLOVILLEGAS@navy.gov
19	800-511-3779	AIDAILOPEZFERRER@navy.gov	00288	AIDA I LOPEZ FERRER	078484990	1,056.06	800-511-3779	AIDAILOPEZFERRER@navy.gov
20	800-512-4283	AIDALNEGRONCANDELARIA@navy.gov	00321	AIDA L NEGRON CANDELARIA	580946332	1,056.06	800-512-4283	AIDALNEGRONCANDELARIA@navy.gov
21	800-512-9830	AIDAMCHEVALIERHUERTAS@navy.gov	00341	AIDA M CHEVALIER HUERTAS	178506728	1,058.94	800-512-9830	AIDAMCHEVALIERHUERTAS@navy.gov
22	800-513-2870	AIDAMNAVEDOMARTINEZ@navy.gov	00347	AIDA M NAVEDO MARTINEZ	178503585	1,060.86	800-513-2870	AIDAMNAVEDOMARTINEZ@navy.gov
23	800-517-2376	ALBERTFALCONNEGRON@navy.gov	00470	ALBERT FALCON NEGRON	149628222	1,069.92	800-517-2376	ALBERTFALCONNEGRON@navy.gov
24	800-517-3372	ALBERTOBAILEYSUAREZ@navy.gov	00473	ALBERTO BAILEY SUAREZ	151505739	1,069.92	800-517-3372	ALBERTOBAILEYSUAREZ@navy.gov
25	800-517-9521	ALBERTOCGARCIAPIZARRO@navy.gov	00493	ALBERTO C GARCIA PIZARRO	580986251	1,069.92	800-517-9521	ALBERTOCGARCIAPIZARRO@navy.gov
26	800-517-4288	ALBERTOFERNANDEZLOPEZ@navy.gov	00476	ALBERTO FERNANDEZ LOPEZ	332803341	1,069.92	800-517-4288	ALBERTOFERNANDEZLOPEZ@navy.gov

Figura 12: Resultados del “JOIN”

4) Se encontraron varios archivos .pdf que contenían correos electrónicos con archivos comprimidos anejados que se entienden fueron los utilizados para cometer phishing y los cuales al abrirlos se instalaba el malware a la computadora de quien lo recibía. Los acusados utilizaban compañías que tenían servicios entre sí. Por ejemplo, CLARO enviando recibo de pago recibido a la compañía automotriz Copart ubicada en Miami (Figura 13) y la compañía de seguro médico BlueCrossBlueShield enviando una invitación para una Convención de Planes Médicos al MedStar Washington Hospital Center en Washington (Figura 14).

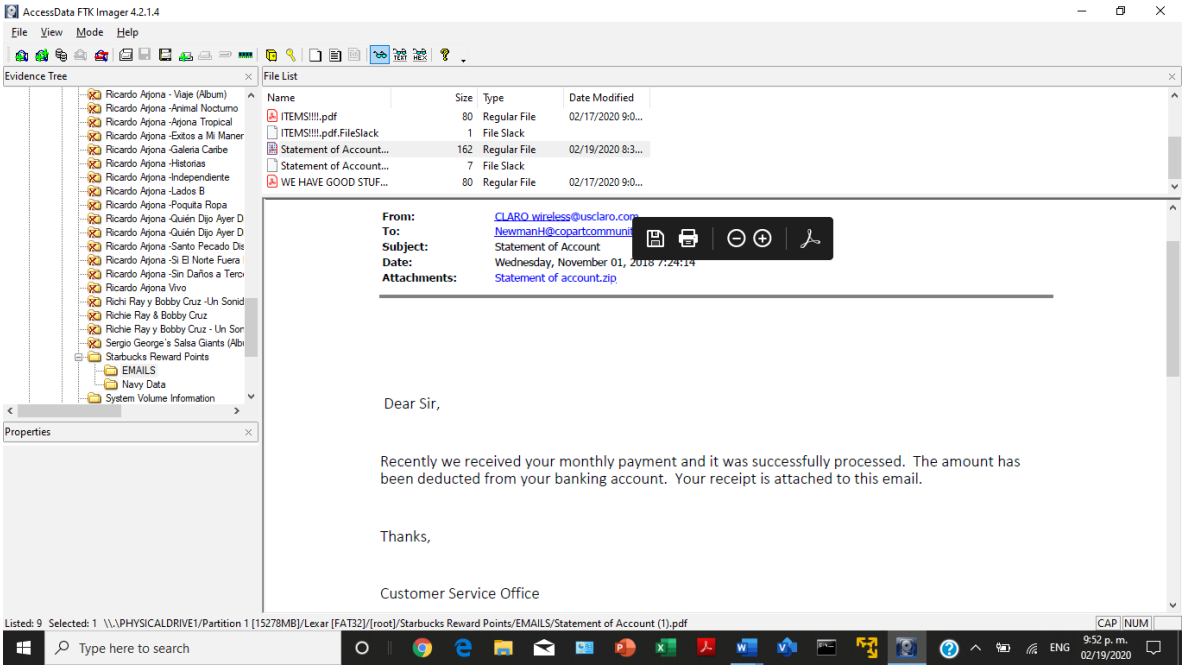


Figura 13: Correo electrónico con archivo comprimido

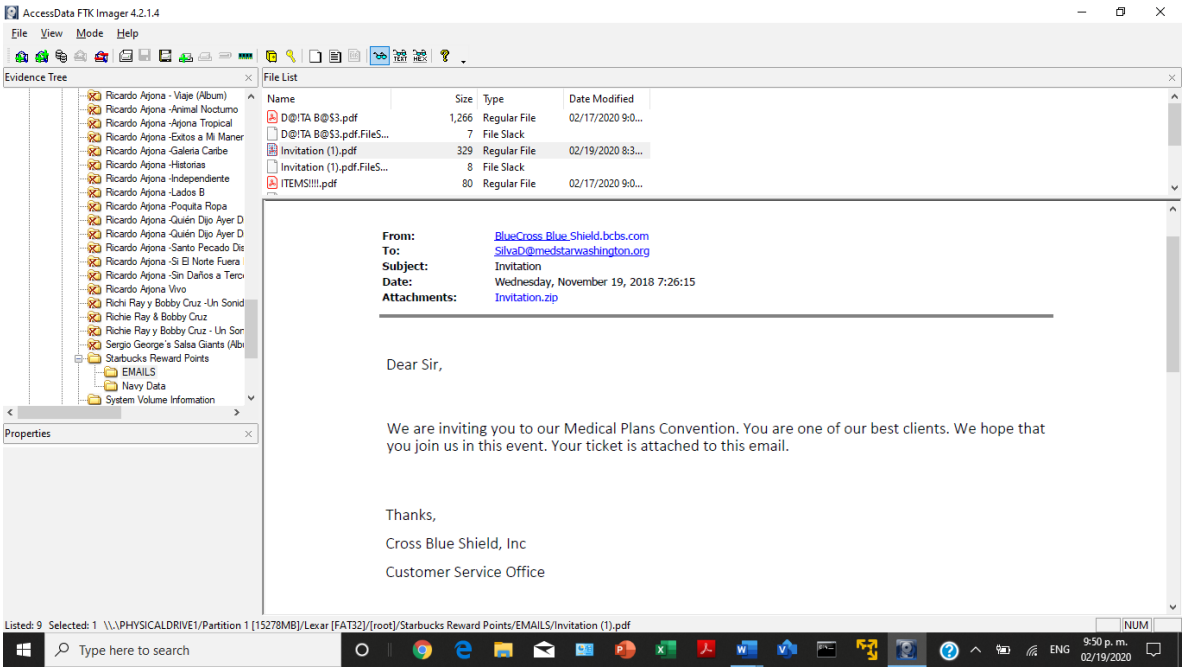


Figura 14: Correo electrónico con archivo comprimido

Cadena de Custodia

La fiscalía federal junto con los investigadores del caso, y el investigador forense digital, Daniel A. Silva, siguieron los protocolos necesarios de acuerdo con el manejo correcto de las evidencias. A continuación, se describirá la cadena de custodia que mostrara el manejo de la información recopilada del caso y como fue la interacción entre el Sr. Silva y los investigadores del caso.

1. **Primer Evento**:

   a. Descripción del Evento: La evidencia fue entregada por el Fiscal Federal Sagar K. Ravi, de la unidad de Fraudes y Ciberdelitos del estado de Nueva York el día 20 de enero de 2019, y fue recibida por Daniel A. Silva, investigador forense digital. La evidencia recibida fue un disco duro de marca Toshiba con número de serie *XD18541C*. El disco está identificado con el número de evidencia E1- 2018-12-20. También se recibió el USB Drive, marca Lexar de 16gb con tag de evidencia E2- 2018-12-20.

   b. Evento verificado por: investigador forense, Daniel A. Silva y el fiscal federal Sagar K. Ravi.

   c. Fecha de comienzo: 20 de enero de 2019 a las 10:15 am

   d. Fecha de terminaci6n: 26 de febrero de 2019 10:40 am

   e. Lugar de origen: Departamento de Justicia Federal en Laboratorio Forense Digital

   f. Destino: Oficina de Investigación Forense Digital de Daniel A. Silva, investigador forense digital.

2. **Segundo Evento**
    a. Descripción del evento: Asignación de numero de caso.
    b. Evento tramitado por: Daniel A. Silva, investigador forense digital.
    c. Numero de caso: IFD-2018-12-20
    d. Fecha de comienzo: 20 de enero de 2019 10:45am
    e. Fecha de terminación: 20 de enero de 2019 11:00am
    f. Lugar de Origen: Oficina de Investigación Forense Digital de Daniel A. Silva, investigador forense digital.
    g. Destino: Oficina de Investigación Forense Digital de Daniel A. Silva, investigador forense digital.
3. **Tercer Evento**
    a. Descripción del evento: Análisis de imagen identificada como "US Digital Forensic Zhu-Zhi Disco Duro" extraída del disco identificado con el número de evidencia E1-2018-12-20. Se utilizó FTK Imager y CaseWare IDEA para el análisis forense digital.
    b. Evento tramitado por: Daniel A. Silva Figueroa, investigador forense digital
    c. Trabajo realizado bajo número de caso: IFD-2018-12-20
    d. Fecha de comienzo: 20 de enero de 2019 12:00 pm
    e. Fecha de terminaci6n: 20 de enero de 2019 9:30 pm
    f. Lugar de origen: Oficina de Investigación Forense Digital de Daniel A. Silva, investigador forense digital
    g. Destino: Oficina de Investigación Forense Digital de Daniel A. Silva, investigador forense digital.

4. Cuarto evento

a. Descripción del evento: Entrega del disco duro identificado como E1-2018-12-20. Este disco fue entregado al Fiscal Federal Sagar K. Ravi por el investigador Daniel A. Silva. También se entregó el informe pericial del caso identificado como IFD-2018-12-20.

b. Evento tramitado por: Daniel A. Silva, investigador forense digital

c. Numero de caso: IFD-2018-12-20

d. Fecha de comienzo: 21 de enero de 2019 2:00 pm

e. Fecha de terminación: 21 de enero de 2019 2:15 pm

f. Lugar de origen: Oficina de Investigación Forense Digital de Daniel A. Silva, investigador forense digital

g. Destino: Laboratorio Forense Digital, Departamento de Justicia Federal

Procedimiento

La investigación forense digital requiere de métodos, estrategias y herramientas de investigación que permitan un buen análisis de los datos. En la misma, durante el proceso de la investigación se ira determinando de acuerdo con el caso, qué herramientas serán utilizadas para la investigación.

A continuación, se describirán los procesos llevados a cabo por parte del investigador forense digital Daniel A. Silva para examinar el archivo de Excel con su metodología. Es muy importante conocer que toda investigación debe tener un nivel de confidencialidad de acuerdo con el tipo de caso.

1. Procedimiento – Preparación para análisis del USB Lexar (16gb), evidencia número E2-2018-12-20 a través de la herramienta FTK Imager

    a. Herramienta: FTK Imager

    b. Fecha de comienzo: 20 de enero de 2019 12:00 pm

    c. Fecha de terminación 20 de enero de 2019 12:15 pm

    d. Descripción del Resultado: Se accedió a la herramienta FTK Imager para analizar el USB buscando posible evidencia sobre los delitos del caso en cuestión

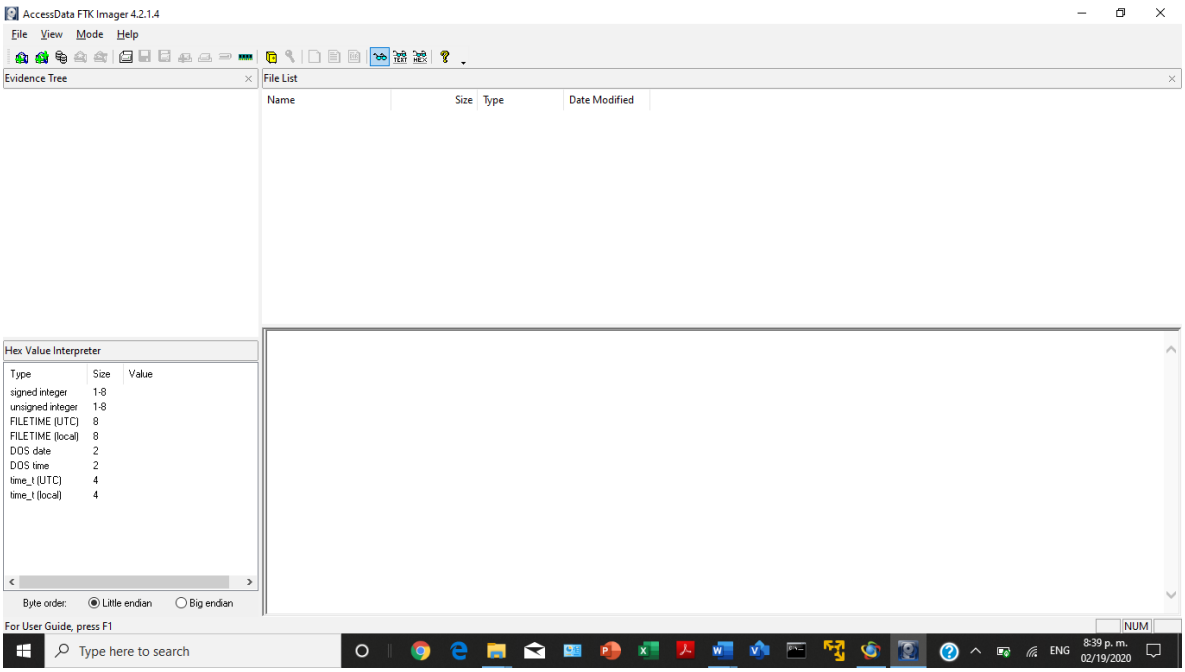


Figura 15: Menú principal del programa FTK Imager

La Figura 16 muestra la evidencia escogida en la herramienta como evidencia. En este caso sería la evidencia física número E2-2018-12-20.

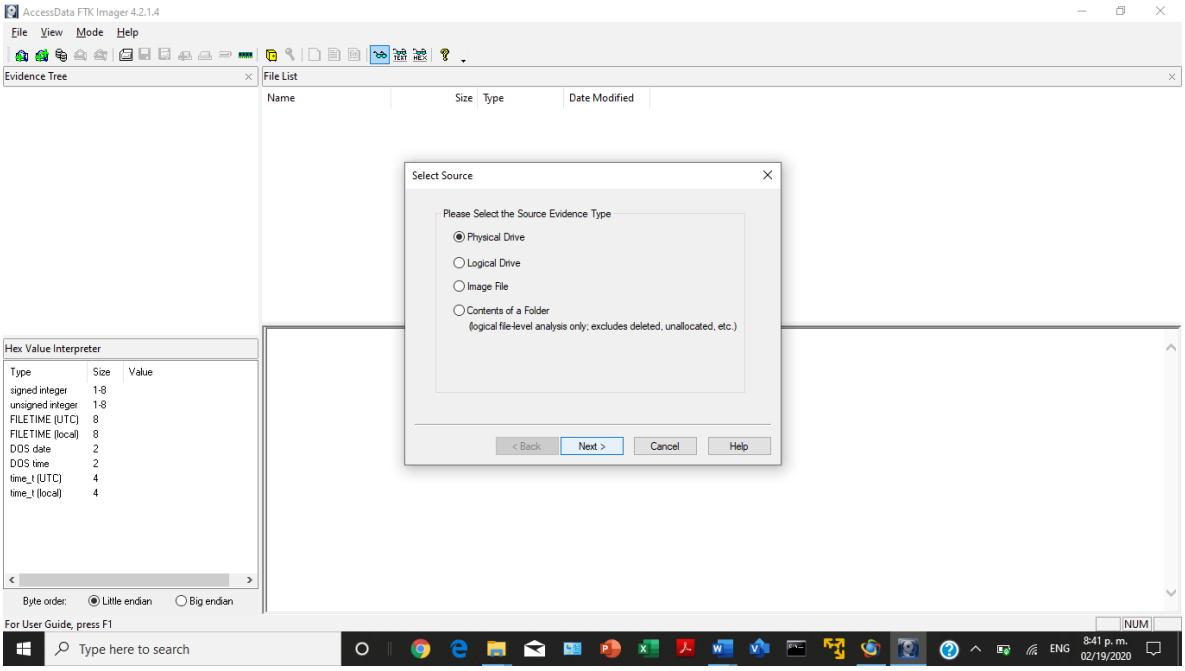


Figura 16: Evidencia escogida para investigar

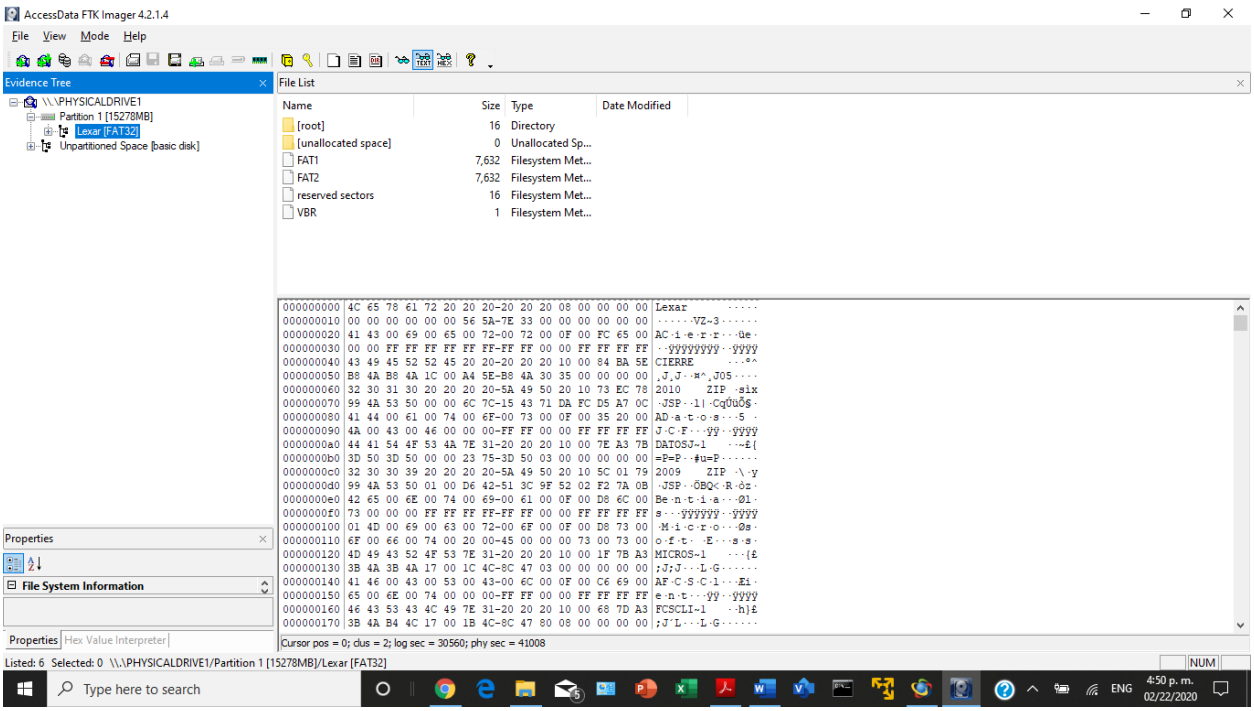


Figura 17: Análisis del USB y sus datos

2. Procedimiento – Análisis de USB Lexar 16gb, evidencia número E2-2018-12-20

    a. Herramienta: FTK Imager

    b. Fecha de comienzo: 20 de enero de 2019 12:30 pm

    c. Fecha de terminación 20 de enero de 2019 3:00 pm

    d. Descripción del Resultado: Se analizaron todos los archivos de la evidencia donde se pudo identificar archivos .pdf que muestran conversaciones de los acusados con el Grupo AP10 y otros correos electrónicos utilizados para cometer phishing relacionados a información de las acusaciones del caso. También se encontró un archivo Excel que muestra una base de datos la cual se relaciona con el robo a datos confidenciales de las Fuerzas Armadas de la Marina (Figura 18-Figura 23).

En la Figura 18 se muestra un email de una conversación entre el acusado y el grupo AP10 donde le notifica que dicho mensaje tiene un documento anejado para vender información. Estos mencionan que tendrán una conversación por Skype a las 7pm y que todos deben estar presentes. El archivo no está anejado en este email.

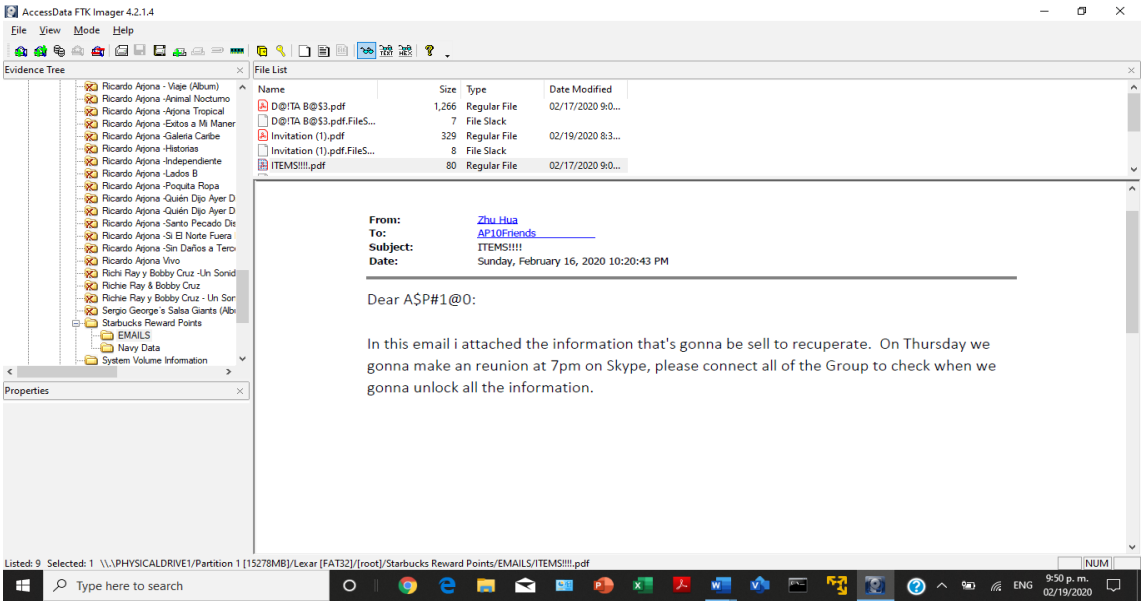


Figura 18: Imagen del correo electrónico entre Zhua Hua con el grupo AP10.

En la Figura 19 se visualiza un archivo .pdf que contiene un correo electrónico entre el acusado Zhu Hua con el grupo AP10 donde el acusado envía como anejo el archivo Excel con los datos antes mencionados y que fue enviado luego del correo electrónico antes mencionado. Este documento presenta evidencia de datos posiblemente robados de las Fuerzas Armadas de la Marina.

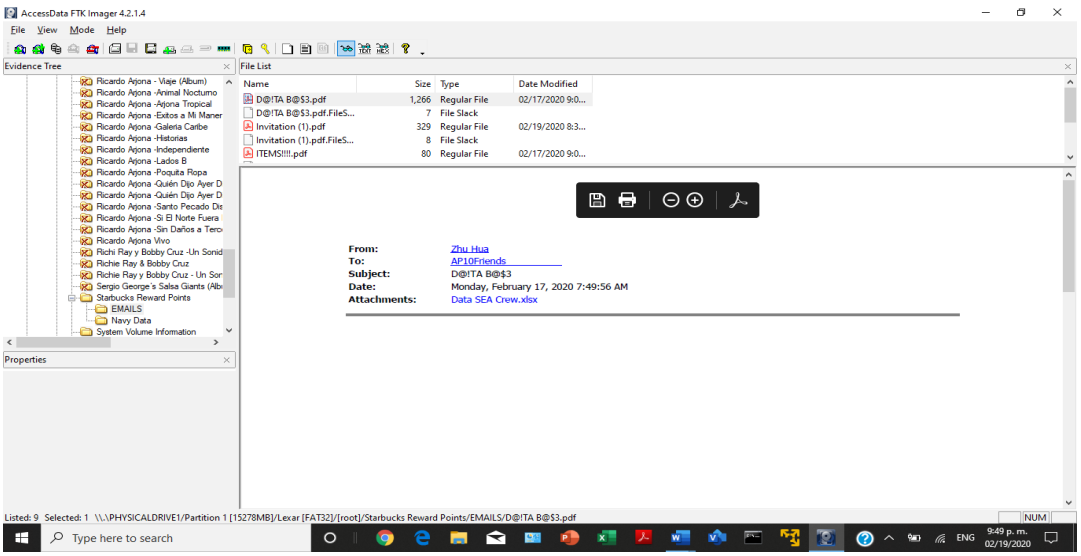
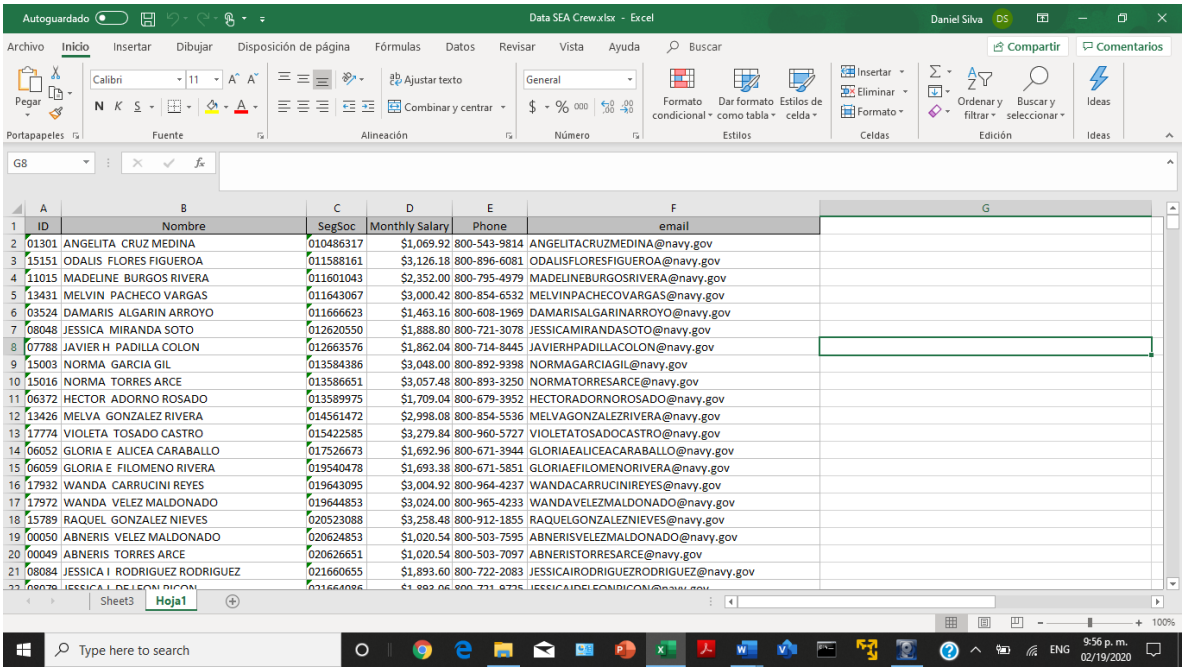


Figura 19: Correo electrónico con archivo Excel

En la Figura 20 se muestra el archivo Excel Data SEA Crew.xls donde se pueden visualizar seis columnas con datos confidenciales que se entiende es la información que fue robada a las Fuerzas Armadas de la Marina.



ID	Nombre	SegSoc	Monthly Salary	Phone	email
01301	ANGELITA CRUZ MEDINA	010486317	$1,069.92	800-543-9814	ANGELITACRUZMEDINA@navy.gov
15151	ODALIS FLORES FIGUEROA	011588161	$3,126.18	800-896-6081	ODALISFLORESFIGUEROA@navy.gov
11015	MADELINE BURGOS RIVERA	011601043	$2,352.00	800-795-4979	MADELINEBURGOSRIVERA@navy.gov
13431	MELVIN PACHECO VARGAS	011643067	$3,000.42	800-854-6532	MELVINPACHECOVARGAS@navy.gov
03524	DAMARIS ALGARIN ARROYO	011666623	$1,463.16	800-608-1969	DAMARISALGARINARROYO@navy.gov
08048	JESSICA MIRANDA SOTO	012620550	$1,888.80	800-721-3078	JESSICAMIRANDASOTO@navy.gov
07788	JAVIER H PADILLA COLON	012663576	$1,862.04	800-714-8445	JAVIERHPADILLACOLON@navy.gov
15003	NORMA GARCIA GIL	013584386	$3,048.00	800-892-9398	NORMAGARCIAGIL@navy.gov
15016	NORMA TORRES ARCE	013586651	$3,057.48	800-893-3250	NORMATORRESARCE@navy.gov
06372	HECTOR ADORNO ROSADO	013589975	$1,709.04	800-679-3952	HECTORADORNOROSADO@navy.gov
13426	MELVA GONZALEZ RIVERA	014561472	$2,998.08	800-854-5536	MELVAGONZALEZRIVERA@navy.gov
17774	VIOLETA TOSADO CASTRO	015422585	$3,279.84	800-960-5727	VIOLETATOSADOCASTRO@navy.gov
06052	GLORIA E ALICEA CARABALLO	017526673	$1,692.96	800-671-3944	GLORIAEALICEACARABALLO@navy.gov
06059	GLORIA E FILOMENO RIVERA	019540478	$1,693.38	800-671-5851	GLORIAEFILOMENORIVERA@navy.gov
17932	WANDA CARRUCINI REYES	019643095	$3,004.92	800-964-4237	WANDACARRUCINIREYES@navy.gov
17972	WANDA VELEZ MALDONADO	019644853	$3,024.00	800-965-4233	WANDAVELEZMALDONADO@navy.gov
15789	RAQUEL GONZALEZ NIEVES	020523088	$3,258.48	800-912-1855	RAQUELGONZALEZNIEVES@navy.gov
00050	ABNERIS VELEZ MALDONADO	020624853	$1,020.54	800-503-7595	ABNERISVELEZMALDONADO@navy.gov
00049	ABNERIS TORRES ARCE	020626651	$1,020.54	800-503-7097	ABNERISTORRESARCE@navy.gov
08084	JESSICA I RODRIGUEZ RODRIGUEZ	021660655	$1,893.60	800-722-2083	JESSICAIRODRIGUEZRODRIGUEZ@navy.gov

Figura 20: Archivo Excel

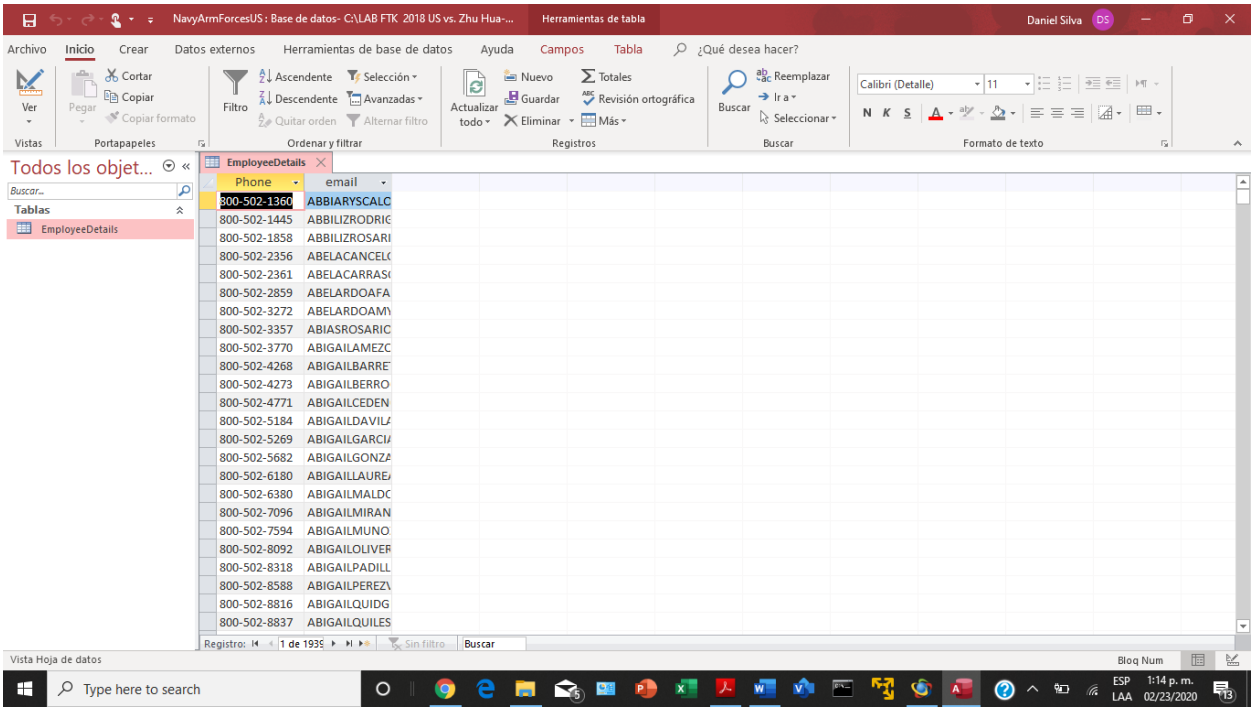


Figura 21: Base de Datos en Access provista por las Fuerzas Armadas.

En la Figura 22 y 23 nos muestra en archivos pdf los correos electrónicos mediante los acusados cometieron el phishing contra las entidades de salud y automovilística. Estos comprimían los documentos que anejaban donde al abrirlos se instalaba el malware en la computadora y tomaban posesión de la misma. Utilizaban correos electrónicos legítimos para dar validez a su mensaje y así la entidad confiar y abrir el documento y ser atacado por el virus.

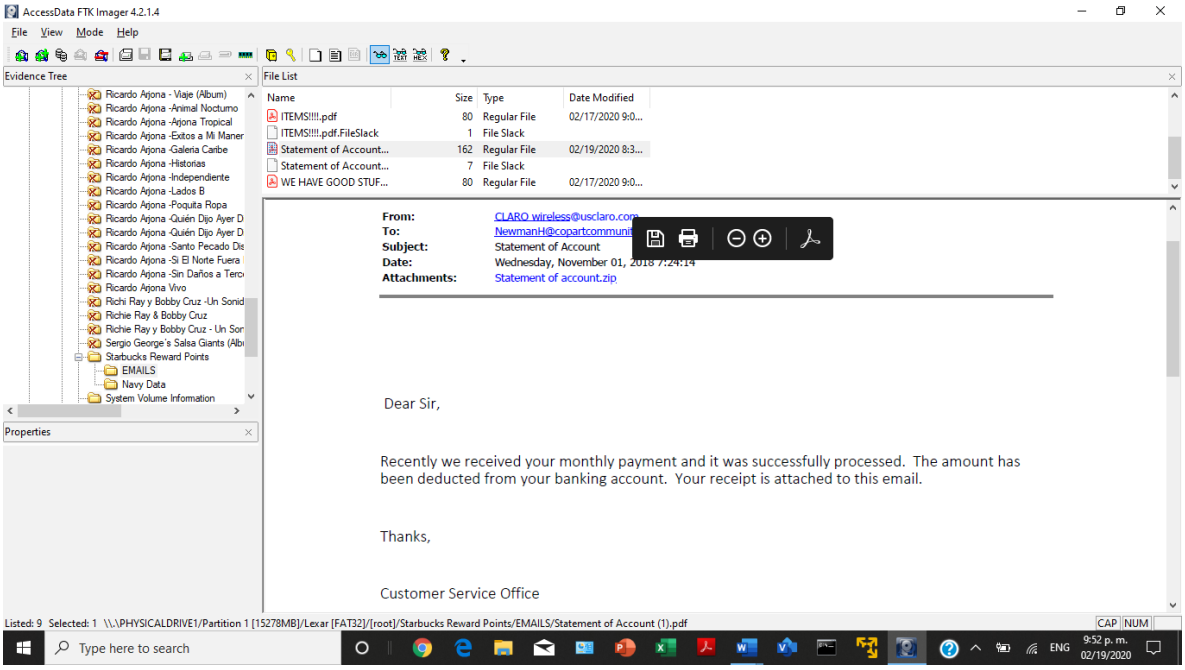


Figura 22: Correo electrónico con archivo comprimido a Automóviles Copart.

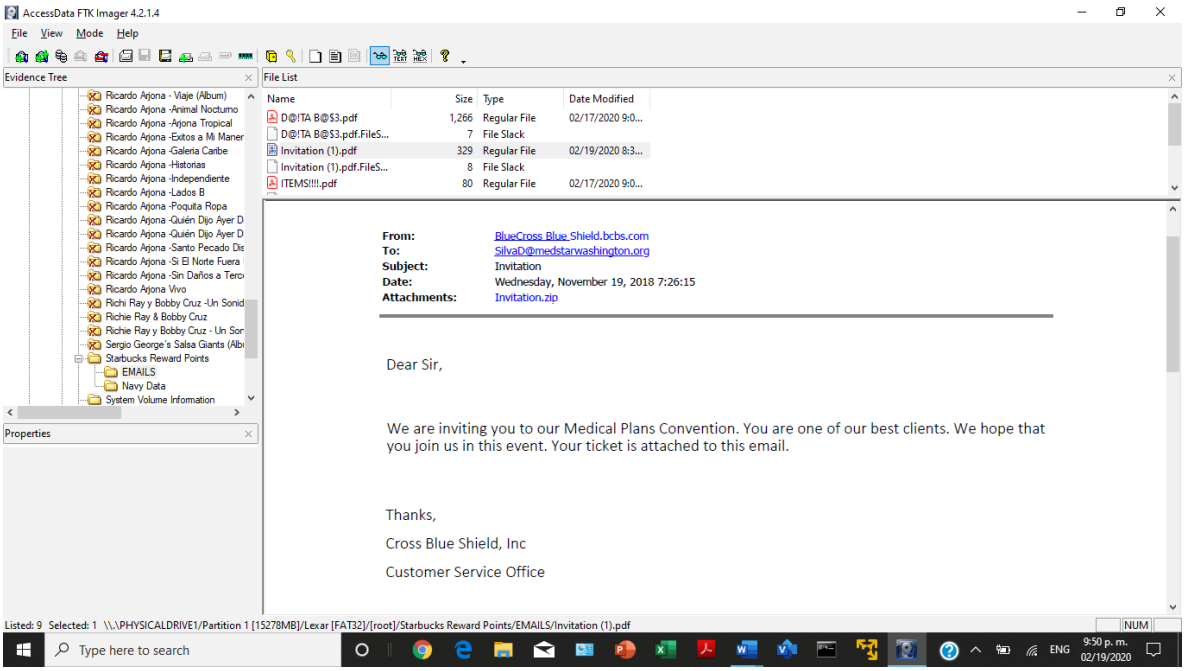


Figura 23: Correo electrónico con archivo comprimido

3. Procedimiento- Preparación para análisis de la base de datos recuperada a través de CaseWare IDEA

    a. Herramienta: CaseWare IDEA

    b. Fecha de comienzo: 20 de enero de 2019 3:00 pm

    c. Fecha de terminación 20 de enero de 2019 3:15 pm

    d. Descripción: Se accedió a la herramienta CaseWare IDEA para analizar las bases de datos obtenidas y ver si se relacionan con los datos recuperados de la computadora de los acusados. La Figura 24 muestra el menú principal de IDEA y la 25 la creación del Proyecto en IDEA.

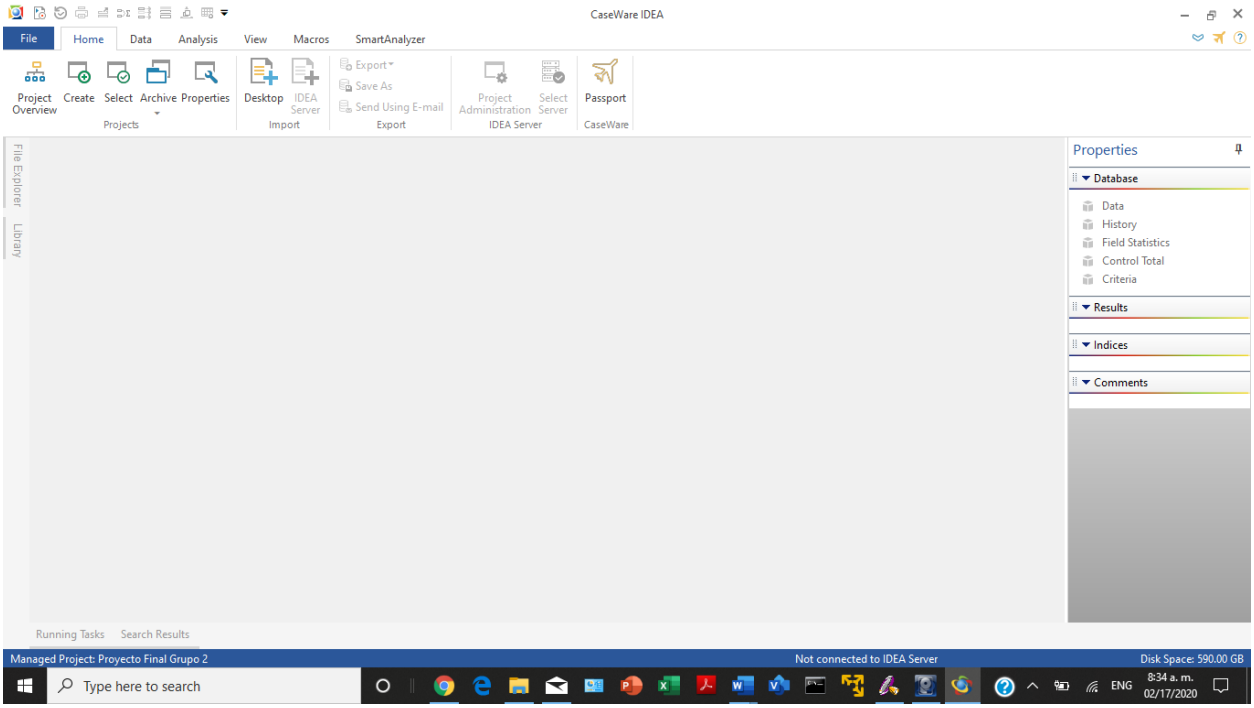


Figura 24: Menú Principal de CaseWare IDEA

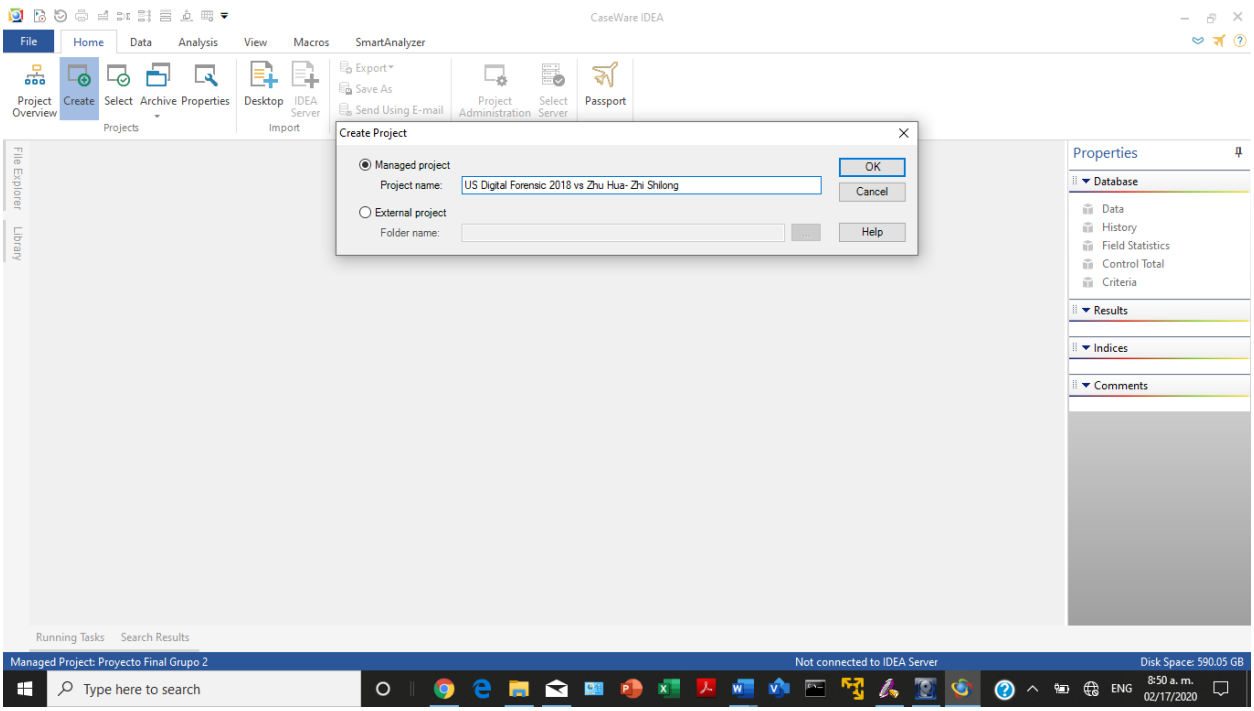


Figura 25: Creación del Proyecto en IDEA

4. Procedimiento: Se realizó la importación de los archivos en Excel incautados a través del análisis con FTK en el USB Drive Lexar(E2-2018-12-20).

   a. Herramienta: CaseWare IDEA

   b. Fecha de comienzo: 20 de enero de 2019 3:30 pm

   c. Fecha de terminación 20 de enero de 2019 5:35 pm

   d. Descripción: Al importar el archivo de Excel obtenido de la evidencia “E2-2018-12-20”, luego se compara utilizando la base de datos oficial recuperada de las Fuerzas Armadas de la Marina de Estados Unidos. La relación se hizo a través de la columna “email” para identificar la perdida de datos durante el fraude cometido (ver Figura 27).

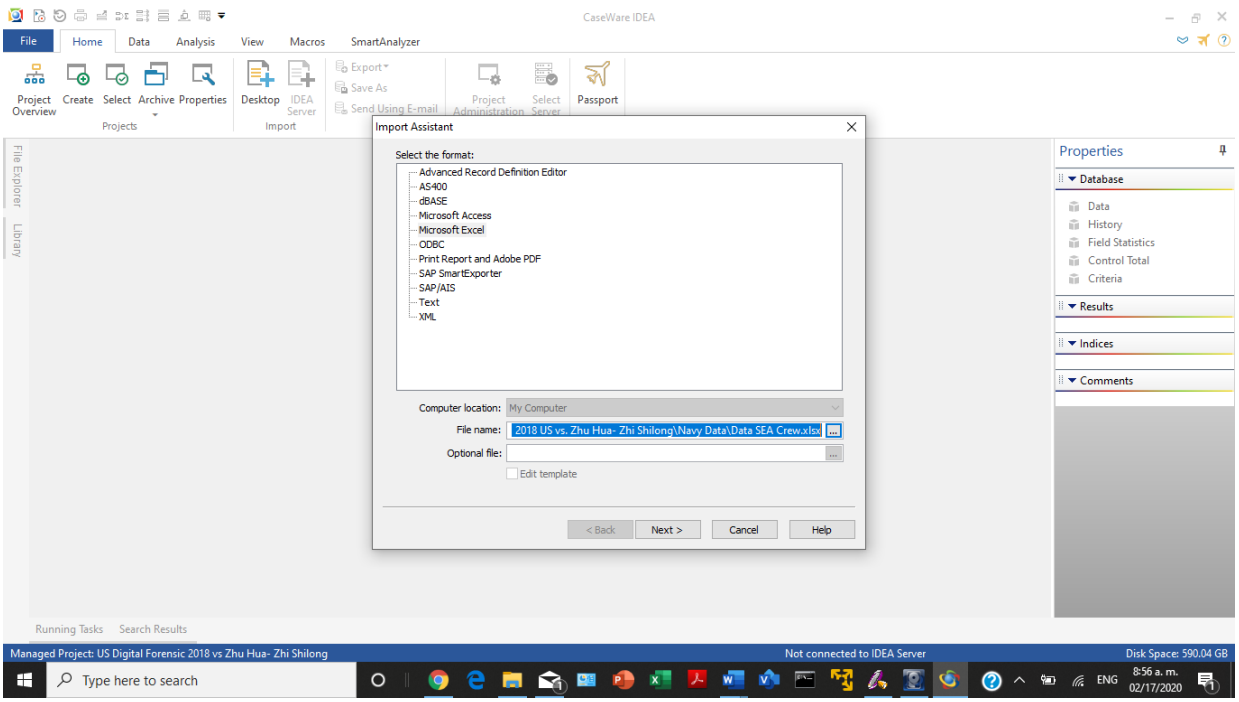


Figura 26: Importe de Base de Datos

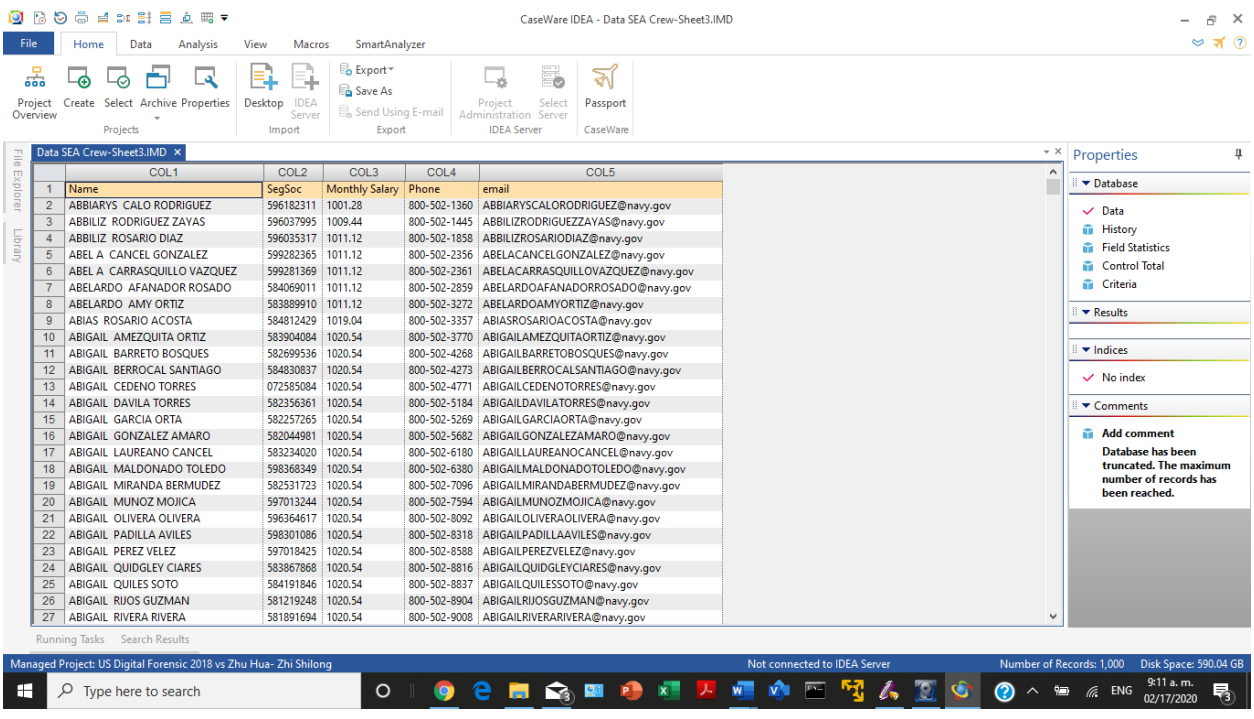


Figura 27: Base de Datos en Excel recuperada de las Fuerzas Armadas de la Marina importada

En la Figura 28 se muestra la base de datos provista por las Fuerzas Armadas de la Marina para verificar y comparar los datos encontrados durante la investigación.

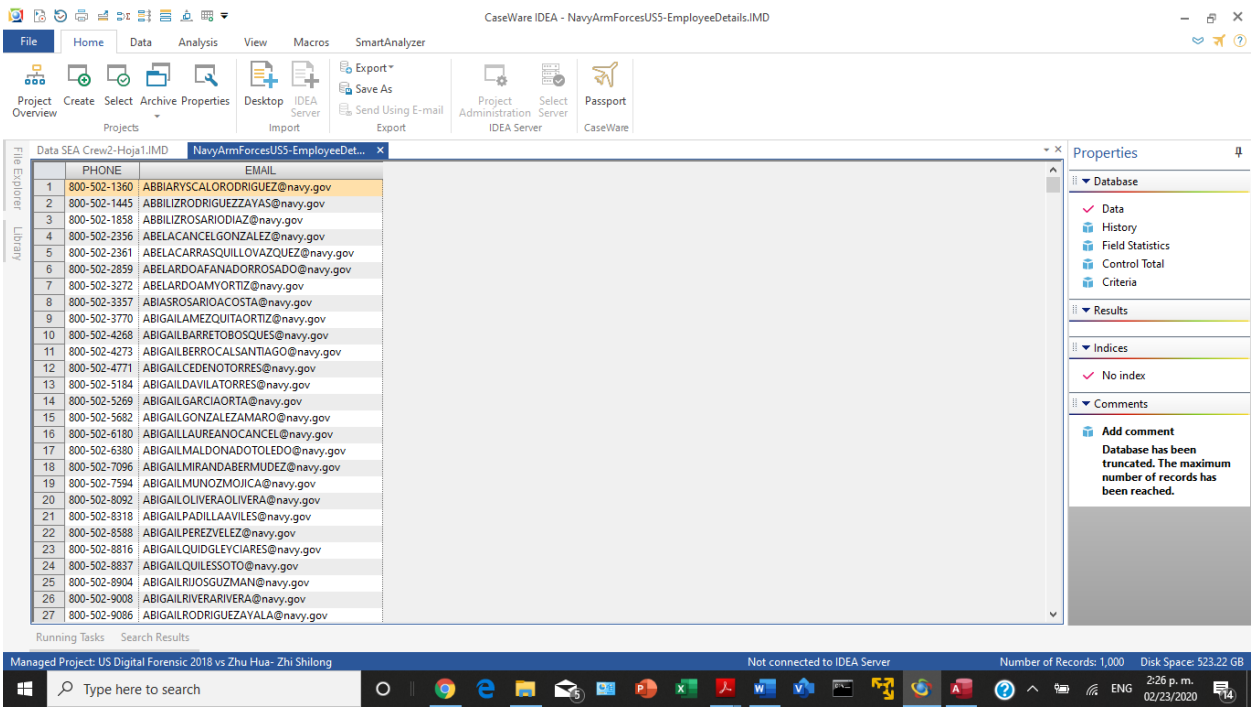


Figura 28: Base de Datos importada

En la Figura 29 muestra cómo se procedió a realizar la función "*Join*" para comparar los campos que contienen los mismos datos y analizar si existe una pérdida de datos.

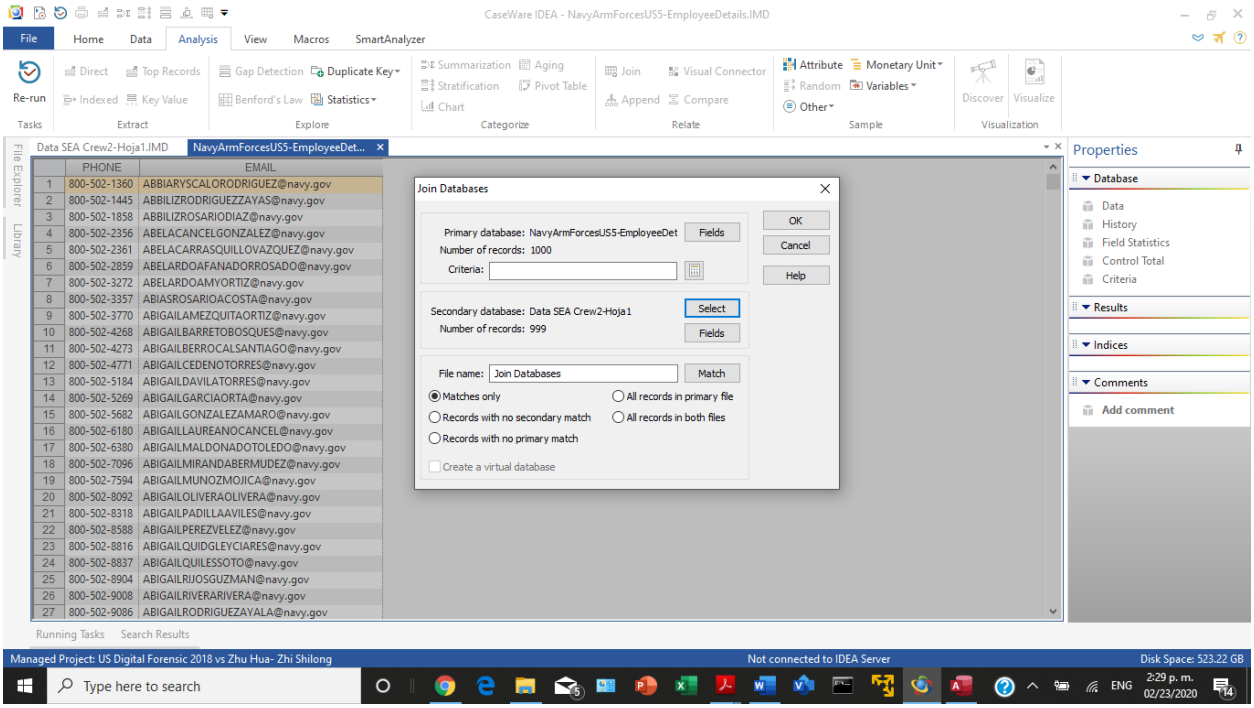
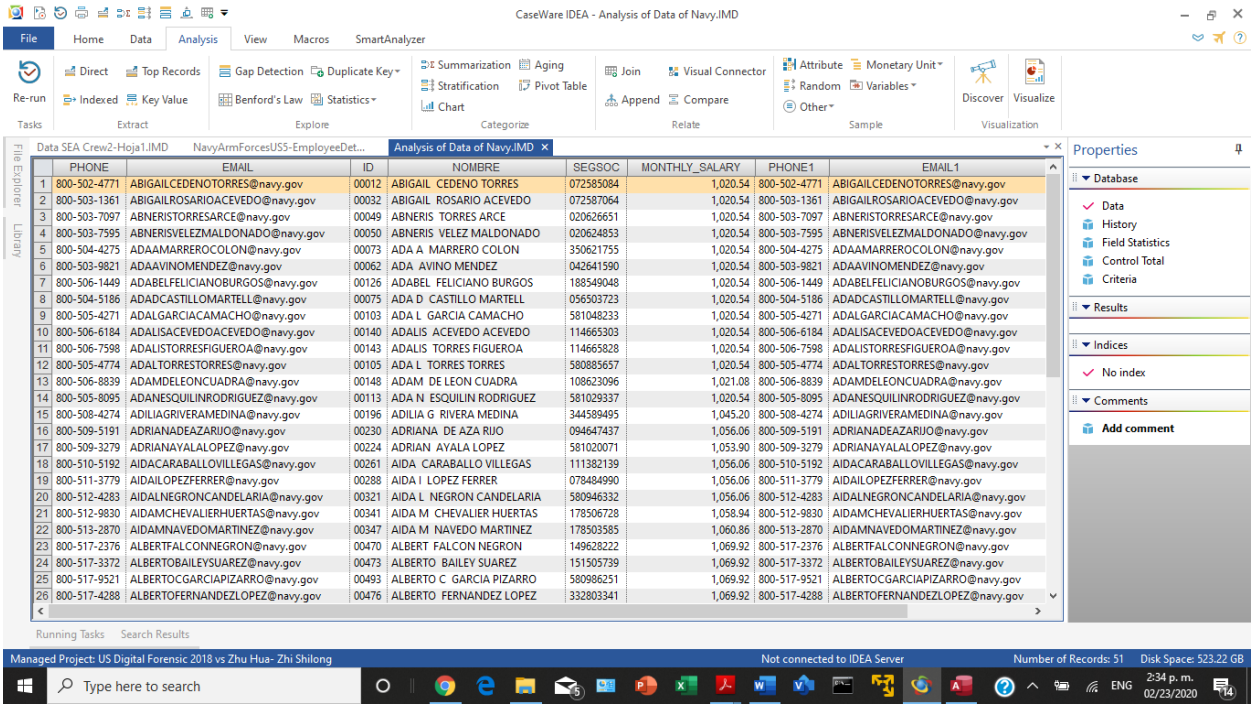


Figura 29: Aplicación de los criterios para "JOIN"

La Figura 30 muestra el resultado luego del "*JOIN*" para unir las bases de datos.



	PHONE	EMAIL	ID	NOMBRE	SEGSOC	MONTHLY_SALARY	PHONE1	EMAIL1
1	800-502-4771	ABIGAILCEDENOTORRES@navy.gov	00012	ABIGAIL CEDENO TORRES	072585084	1,020.54	800-502-4771	ABIGAILCEDENOTORRES@navy.gov
2	800-503-1361	ABIGAILROSARIOACEVEDO@navy.gov	00032	ABIGAIL ROSARIO ACEVEDO	072587064	1,020.54	800-503-1361	ABIGAILROSARIOACEVEDO@navy.gov
3	800-503-7097	ABNERISTORRESARCE@navy.gov	00049	ABNERIS TORRES ARCE	020626651	1,020.54	800-503-7097	ABNERISTORRESARCE@navy.gov
4	800-503-7595	ABNERISVELEZMALDONADO@navy.gov	00050	ABNERIS VELEZ MALDONADO	020624853	1,020.54	800-503-7595	ABNERISVELEZMALDONADO@navy.gov
5	800-504-4275	ADAAMARRERCOLON@navy.gov	00073	ADA A MARRERO COLON	350621755	1,020.54	800-504-4275	ADAAMARRERCOLON@navy.gov
6	800-503-9821	ADAAVINOMENDEZ@navy.gov	00062	ADA AVINO MENDEZ	042641590	1,020.54	800-503-9821	ADAAVINOMENDEZ@navy.gov
7	800-506-1449	ADABELFELICIANOBURGOS@navy.gov	00126	ADABEL FELICIANO BURGOS	188549048	1,020.54	800-506-1449	ADABELFELICIANOBURGOS@navy.gov
8	800-504-5186	ADADCASTILLOMARTELL@navy.gov	00075	ADA D CASTILLO MARTELL	056503723	1,020.54	800-504-5186	ADADCASTILLOMARTELL@navy.gov
9	800-505-4271	ADALGARCIACAMACHO@navy.gov	00103	ADA L GARCIA CAMACHO	581048233	1,020.54	800-505-4271	ADALGARCIACAMACHO@navy.gov
10	800-506-6184	ADALISACEVEDOACEVEDO@navy.gov	00140	ADALIS ACEVEDO ACEVEDO	114665303	1,020.54	800-506-6184	ADALISACEVEDOACEVEDO@navy.gov
11	800-506-7598	ADALISTORRESFIGUEROA@navy.gov	00143	ADALIS TORRES FIGUEROA	114665828	1,020.54	800-506-7598	ADALISTORRESFIGUEROA@navy.gov
12	800-505-4774	ADALTORRESTORRES@navy.gov	00105	ADA L TORRES TORRES	580885657	1,020.54	800-505-4774	ADALTORRESTORRES@navy.gov
13	800-506-8839	ADAMDELEONCUADRA@navy.gov	00148	ADAM DE LEON CUADRA	108623096	1,021.08	800-506-8839	ADAMDELEONCUADRA@navy.gov
14	800-505-8095	ADANESQUILINRODRIGUEZ@navy.gov	00113	ADA N ESQUILIN RODRIGUEZ	581029337	1,020.54	800-505-8095	ADANESQUILINRODRIGUEZ@navy.gov
15	800-508-4274	ADILIAGRIVERAMEDINA@navy.gov	00196	ADILIA G RIVERA MEDINA	344589495	1,045.20	800-508-4274	ADILIAGRIVERAMEDINA@navy.gov
16	800-509-5191	ADRIANADEAZARIJO@navy.gov	00230	ADRIANA DE AZA RIJO	094647437	1,056.06	800-509-5191	ADRIANADEAZARIJO@navy.gov
17	800-509-3279	ADRIANAYALALOPEZ@navy.gov	00224	ADRIAN AYALA LOPEZ	581020071	1,053.90	800-509-3279	ADRIANAYALALOPEZ@navy.gov
18	800-510-5192	AIDACARABALLOVILLEGAS@navy.gov	00261	AIDA CARABALLO VILLEGAS	111382139	1,056.06	800-510-5192	AIDACARABALLOVILLEGAS@navy.gov
19	800-511-3779	AIDAILOPEZFERRER@navy.gov	00288	AIDA I LOPEZ FERRER	078484990	1,056.06	800-511-3779	AIDAILOPEZFERRER@navy.gov
20	800-512-4283	AIDALNEGRONCANDELARIA@navy.gov	00321	AIDA L NEGRON CANDELARIA	580946332	1,056.06	800-512-4283	AIDALNEGRONCANDELARIA@navy.gov
21	800-512-9830	AIDAMCHEVALIERHUERTAS@navy.gov	00341	AIDA M CHEVALIER HUERTAS	178506728	1,058.94	800-512-9830	AIDAMCHEVALIERHUERTAS@navy.gov
22	800-513-2870	AIDAMNAVEDOMARTINEZ@navy.gov	00347	AIDA M NAVEDO MARTINEZ	178503585	1,060.86	800-513-2870	AIDAMNAVEDOMARTINEZ@navy.gov
23	800-517-2376	ALBERTFALCONNEGRON@navy.gov	00470	ALBERT FALCON NEGRON	149628222	1,069.92	800-517-2376	ALBERTFALCONNEGRON@navy.gov
24	800-517-3372	ALBERTOBAILEYSUAREZ@navy.gov	00473	ALBERTO BAILEY SUAREZ	151505739	1,069.92	800-517-3372	ALBERTOBAILEYSUAREZ@navy.gov
25	800-517-9521	ALBERTOCGARCIAPIZARRO@navy.gov	00493	ALBERTO C GARCIA PIZARRO	580986251	1,069.92	800-517-9521	ALBERTOCGARCIAPIZARRO@navy.gov
26	800-517-4288	ALBERTOFERNANDEZLOPEZ@navy.gov	00476	ALBERTO FERNANDEZ LOPEZ	332803341	1,069.92	800-517-4288	ALBERTOFERNANDEZLOPEZ@navy.gov

Figura 30: Resultados obtenidos

Conclusión

El proceso del análisis forense realizado para la obtención de la evidencia del caso nos muestra como los acusados poseían datos los cuales no deberían encontrarse en su disco duro. Los correos electrónicos muestran que estos guardan relación con los delitos por los cuales son acusados Zhu Hua y Zhang Shilong, ya que estos mismos correos electrónicos, por ejemplo, el enviado de la empresa Blue Shield Blue Cross a el MedStar Washington Hospital. También se encontró que el archivo en Excel recuperado en la investigación guarda relación con la base de datos de las Fuerzas Armadas de la Marina. La cadena de Custodia llevada a cabo por el investigador forense Daniel A. Silva, muestra claramente el proceso y manejo de la evidencia. El mismo, fue regido bajo los parámetros establecidos en los Estados Unidos, donde se encuentran siendo procesados.

Sección 5: Discusión del Caso

El fraude impacto a cada una de las victimas ya que los acusados robaron información sensible y confidencial incluyendo empresas gubernamentales de Estados Unidos y otros países del Mundo. Los acusados, Zhang Shilong y Zhu Hua trabajaban con Advanced Persistent Threat 10 (el Grupo APT10) y estaban asociados con la Oficina de Seguridad del Estado de Tianjin del Ministerio de Seguridad del Estado de China. Estos realizaron campañas globales de intrusiones informáticas dirigidas, entre otros datos, propiedad intelectual e información comercial y tecnológica confidencial en el servicio administrado proveedores (MSP), que son empresas que administran de forma remota la infraestructura de tecnología de la información de empresas y gobiernos de todo el mundo, más de 45 empresas de tecnología en al menos una docena de estados de EE. UU. y agencias gubernamentales de EE. UU. El Grupo APT10 se centró en una amplia gama de actividades comerciales, industrias y tecnologías, incluida la aviación, tecnología satelital y marítima, automatización de fábricas industriales, suministros automotrices, instrumentos de laboratorio, banca y finanzas, telecomunicaciones y electrónica de consumo, tecnología de procesador de computadoras, servicios de tecnología de la información, embalaje, consultoría, equipos médicos, atención médica, biotecnología, fabricación farmacéutica, minería y exploración y producción de petróleo y gas. Entre otras cosas, Zhu y Zhang registraron la infraestructura de TI que el Grupo APT10 usó para sus intrusiones y participó en operaciones de piratería ilegal. A través de sus acciones durante los años el grupo y los acusados piratearon computadoras en al menos una docena de países y le dio acceso al servicio de inteligencia de China a información comercial confidencial (US Dpt. of Justice, 2018).

Con relación al Navy, los acusados pudieron haber utilizados los datos de las víctimas, por ejemplo, utilizando sus correos electrónicos para cometer phishing, podrían utilizar su seguro

social donde robando la identidad de las victimas podrían cometer fraudes a nombre de la persona. Con relación a las compañías a las cuales fueron comprometidas sus computadoras con el malware enviado por los acusados tendrán que invertir ya sea para nuevas computadoras o sistemas de protección para ser menos vulnerables a ser atacados.

Sección 6. Informe de Auditoria y Prevención

Trasfondo

ZHUA y ZHANG SHILONG los acusados, ambos quienes eran nacionales de la República Popular de China ("China"), eran miembros de un grupo de piratería que operaba en China, conocido dentro de la comunidad de seguridad cibernética como el "Grupo APTlO" (Advanced Persistent Threat 10). Estos son acusados por desde o alrededor de 2006 hasta alrededor del 2018, por robar tecnologías y otra información de valor para la conspiración. Los acusados trabajaron para la Compañía de Desarrollo de Ciencia y Tecnología Huaying Haitai ("Huaying Haitai") en Tianjin, China, y actuaron en asociación con la Oficina de Seguridad del Estado de Tianjin del Ministerio de Seguridad del Estado de China. Los miembros del Grupo APTlO trabajaban en un entorno de oficina y generalmente se dedicaban a piratear operaciones durante el horario laboral en China. La información comprometida incluía compañías que estaban involucradas en una amplia gama de actividades comerciales, industriales y tecnológicas, incluyendo banca y finanzas, telecomunicaciones y electrónica de consumo, equipos médicos, empaques, manufactura, consultoría, atención médica, biotecnología, automotriz, petróleo y gas. exploración y minería.

Alcance

El alcance de esta auditoria es examinar detalladamente los datos registrados en la base de datos de las Fuerzas Armadas de la Marina de Estados Unidos y los datos encontrados de evidencia. Además, se analizará la forma en que fueron atacadas las empresas para evaluar los controles existentes y si se deben mejorar para aumentar la confiabilidad de la data. Se comprobará si las empresas y/o personas víctimas de los acusados fueron proactivas en la utilización del Internet y sus sistemas para evitar el fraude.

Objetivo

El objetivo de esta auditoria es mantener los controles necesarios para prevenir los riesgos de los ataques cibernéticos, sobre todo, los que ocurrieron en este caso: Phishing, robo de identidad e instalación de malware.

Hallazgos

1. Hallazgo: Falta de controles en la seguridad no encriptando los datos y así permitiendo acceso a la base de datos de las Fuerzas Armadas de la Marina, provocando el robo de información sensible de su personal.
    a) Condición: La evidencia demostró que el archivo Excel eran datos que incluían nombre, seguro social, salarios, teléfonos, emails, entre otros de las Fuerzas Armadas de la Marina.
    b) Criterio: Si hubiesen existido los controles necesarios, las computadoras no hubiesen sido comprometidas con toda esa información confidencial del Navy.
    c) Causa: La condición fue causada por la falla del control de la seguridad de la información que permitió que los acusados presuntamente tomaran posesión de las computadoras.
    d) Efecto: El impacto en la organización fue el que se comprometió sobre 100,000 datos de personal de las Fuerzas Armadas de la Marina, aunque no se perdió la data. En este caso hubo riesgo del robo de identidad.
2. Hallazgo: Falta de controles en la base de datos del proveedor de internet MSP de las compañías las cuales recibían el servicio. Al tomar posesión de datos de las diferentes compañías, a través de los correos electrónicos tomaban posesión de las computadoras instalando el malware para así robar la información.

a. Condición: Se encontraron varios correos electrónicos que parecían legítimos y que contenían archivos comprimidos que presuntamente fueron enviados. Estos al abrirlos, automáticamente instalaban el malware y así tomaban posesión de la computadora, adquiriendo la información necesaria para cometer el fraude.
b. Criterio: Si hubiesen existido los controles necesarios, los *"hackers"* nunca debieron haber podido tener acceso a las bases de datos del MSP.
c. Causa: Ausencia de controles
d. Efecto: El mayor impacto fue la perdida de información, ya que según los delitos por los cuales son acusados, China tomaba esta información valiosa, la que usaba a su favor económicamente.

3. Hallazgo: No existía controles ni ningún tipo de software el cual identifique posibles ataques de phishing en el correo electrónico.
   a. Condición: La evidencia demostró que a estos cometer el fraude mediante el phishing las víctimas no contenían un software el cual previniera o notificara el ataque.
   b. Criterio: Si hubiesen existido los controles necesarios, los *"hackers"* no hubiesen tenido el acceso.
   c. Causa: Ausencia de controles
   d. Efecto: El mayor impacto fue la perdida de información, ya que según los delitos por los cuales son acusados, China tomaba esta información valiosa, la que usaba a su favor económicamente.

Recomendaciones

1) Revisar los controles que se tienen para acceder los datos del MSP y los controles de seguridad verificando vulnerabilidades en el sistema e intentos de intrusiones.
2) Otra recomendación es adiestrar al personal de cómo identificar posibles correos sospechosos para así evitar ser atacados.
3) Que las compañías instalen un software, ya sea antivirus, de acuerdo a su nivel de sensibilidad de su información, para así protegerse de ser atacados.

Sección 7: Conclusión

Durante la investigación del caso se pudo conocer el impacto que puede provocar los fraudes informáticos tanto a nivel gubernamental como también a nivel de individuo. Se pudo observar cómo los acusados en conjunto con el Grupo AP10 se mantuvieron cometiendo fraudes por 12 años (2006-2018) sin ser detenidos. Así también queda demostrado que los avances tecnológicos nos hacen más vulnerables a los fraudes, al robo de identidad y a la perdida de capital. Es importante que tanto a nivel individual como empresarial nos mantengamos al día con los conocimientos tecnológicos y las diferentes técnicas que están utilizando los delincuentes para cometer fraude. Solo tiene que existir una falla para que un intruso la detecte y se aproveche de la misma para cometer el delito.

Se pudo analizar en este caso la falta de controles y software que contenían esas agencias tanto gubernamentales como privadas. Con el tan solo no conocer lo que es un spearfishing te hace más vulnerable ya que puedes ser engañado mediante estos correos electrónicos. Es importante mantener el monitoreo y contener metodologías actualizadas para combatir el fraude según lo necesite la compañía o individuo.

Estos formaron parte de campañas globales de intrusiones informáticas dirigidas, entre otros datos, propiedad intelectual e información comercial y tecnológica confidencial en el servicio administrado proveedores (MSP), que son empresas que administran de forma remota la infraestructura de tecnología de la información de empresas y gobiernos de todo el mundo, más de 45 empresas de tecnología en al menos una docena de estados de EE. UU. y agencias gubernamentales de EE. UU.

A través de dicha investigación se logró conocer cuan rigurosas son las leyes r de acuerdo con el fraude cibernético. Se obtuvo el conocimiento necesario para poder identificar y evitar ser víctima de phishing a nivel personal donde en muchas ocasiones con el ajoro del día a día no nos percatamos de cuan poderoso son herramientas como el celular. Gracias a esta investigación pude aplicar todos los conocimientos adquiridos durante la maestría utilizando las herramientas brindadas en cada curso para así poder realizar una investigación correctamente.

Sección 8: Referencias

18 u.s. Code § 1028a - aggravated identity theft. (s.f.). Recuperado de https://www.law.cornell.edu/uscode/text/18/1028A

18 u.s. Code § 1030 - fraud and related activity in connection with computers. (s.f.). Recuperado de https://www.law.cornell.edu/uscode/text/18/1030

18 u.s. Code § 1343 - fraud by wire, radio, or television. (s.f.). Recuperado de https://www.law.cornell.edu/uscode/text/18/1343

18 u.s. Code § 1349 - attempt and conspiracy. (s.f.). Recuperado de https://www.law.cornell.edu/uscode/text/18/1349

18 u.s. Code § 3238 - offenses not committed in any district. (s.f.). Recuperado de https://www.law.cornell.edu/uscode/text/18/3238

Albors, J. (2015). Phishing, exploits y botnets: ¿cómo pueden afectar a las empresas? | welivesecurity. Recuperado de https://www.welivesecurity.com/la-es/2015/02/25/phishing-exploits-y-botnets-afectar-empresas/.

Avast. (s.f.). ¿qué es phishing? Recuperado de https://www.avast.com/es-es/c-phishing

Avast. (s.f.). ¿qué es un malware? Recuperado de https://www.avast.com/es-es/c-malware.

Bulk-extractor. (s.f.). Recuperado de https://tools.kali.org/forensics/bulk-extractor.

Cano Francisco. (2014). Definición de piratería. Recuperado de https://www.definicionabc.com/tecnologia/pirateria. php.

Cobb, S. (2019). Cibercrimen: un problema que empeora y que exige actuar cuanto antes | welivesecurity. Recuperado de https://www.welivesecurity.com/la-es/2019/07/16/cibercrimen-problema-empeora-exige-actuar-cuanto-ant es/.

Computer and internet fraud. (s.f.). Recuperado de https://www.law.cornell.edu/wex/computer_and_inter net_fraud

DOJ (2018). Two chinese hackers associated with the ministry of state security charged with global computer intrusion campaigns targeting intellectual property and confidential business information. Recuperado de https://www.justice.gov/opa/pr/two-chinese-hackers -associated-ministry-state-security-charged-global -computer-intrusion.

DOJ. (2018). North korean regime-backed programmer charged with conspiracy to conduct multiple cyber-attacks and intrusions. Recuperado de https://www.justice.gov/opa/pr/north-korean-regime -backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

DOJ. (2019). Former seattle tech worker indicted on federal charges for wire fraud and computer data theft. Recuperado dehttps://www.justice.gov/usao-wdwa/pr/former-seattl e-tech-worker-indicted-federal-charges-wire-fraud- and-computer-data-theft.

El hacker ruso Levashov se declara culpable en EE.UU. de fraude informático. (2018). Recuperado de https://www.efe.com/efe/usa/sociedad/el-hacker-rus o-levashov-se-declara-culpable-en-eeuu-de-fraude-i nformatico/50000101-3747771

Ethics Global. (2016). Robo de información confidencial. Recuperado de https://blog.ethicsglobal.com/robo-de-informacion- confidencial/.

Fraude cibernético e informático. (s.f.). Recuperado de https://www.law.cornell.edu/wex/es/fraude_cibernético_e_informático

Garatu, G. (2019). Ciberdelincuencia: el fraude en el sector de las telecomunicaciones (telecom fraud). Recuperado de https://grupogaratu.com/fraude-sector-de-telecomunicaciones-telecom-fraud-ciberdelincuencia/.

GUIA SOLUCIONES TIC. (s.f.). Recuperado de https://www.guiadesolucionestic.com/sistemas-de-informacion/sistemas-de-soporte-de-deciciones-dss/auditoria-administracion-del-riesgo/1896-idea.

Jaimovich, D. (2018). Cómo surgió y se propagó wannacry, uno de los ciberataques más grandes de la historia. Recuperado de https://www.infobae.com/america/tecno/2018/05/12/como-surgio-y-se-propago-wannacry-uno-de-los-cibera taques-mas-grandes-de-la-historia/.

NESSUS (s.f.) Recuperado de https://es-la.tenable.com/products/nessus.

Quanti Solutions. (2018). Espionaje Informático, robo de identidad e información. Recuperado de https://www.quanti.com.mx/2018/03/05/espionaje-informatico-robo-identidad-e-informacion/.

Qué es el acceso remoto (s.f.) Recuperado de: https://www.citrix.com/es-mx/glossary/what-is-remo te-access.html

Qué es el robo de identidad (s.f.). Recuperado de https://www.abogado.com/recursos/ley-criminal/robo -de-identidad/el-robo-de-identidad.html

Recovery Labs (s.f.) Peritaje Informático - Estadísticas. Recuperado de: https://www.delitosinformaticos.info/peritaje_informatico/estadisticas.html.

Rizaldos. (2018). Qué es metasploit framework Recuperado de https://openwebinars.net/blog/que-es-metasploit/.

Significado de fraude. (2015). Recuperado de https://www.significados.com/fraude/.

Significado de seguridad informática. (2019). Recuperado de https://www.significados.com/seguridad-informatica /.

United States V. Zhu Hua Indicment. (2018). Recuperado de https://www.justice.gov/opa/press-release/file/112 1706/download.

Vaca, Monica. (2020). Los principales fraudes de 2019. Recuperado de https://www.consumidor.ftc.gov/blog/2020/01/los-pr incipales-fraudes-de-2019.

VIU. (2018). ¿qué es la seguridad informática y cómo puede ayudarme? Recuperado de https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/.

whatis.com. (2017) ¿qué es proveedor de servicios gestionados (msp)? - . Recuperado de: https://searchdatacenter.techtarget.com/es/definic ion/Proveedor-de-servicios-gestionados-MSP.

Witt, Paul. (2019). Los principales fraudes de 2018. Recuperado de https://www.consumidor.ftc.gov/blog/2019/02/los-pr incipales-fraudes-de-2018.