

EDP UNIVERSITY OF PUERTO RICO INC.

RECINTO DE HATO REY

ESCUELA GRADUADA

PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACION CON ESPECIALIDAD EN SEGURIDAD  
DE INFORMACIÓN E INVESTIGACIÓN DE FRAUDE

FEDIR HLADYR Y FIN7: IMPACTO A LA INDUSTRIA DE SERVICIOS

FRANCISCO A. MUÑOZ LOPEZ

DICIEMBRE 2019

PROF. MIGUEL A. DROUYN MARRERO, Ed.D., CISA, CFE

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

FEDIR HLADYR Y FIN7: IMPACTO A LA INDUSTRIA DE SERVICIOS

Preparado por

Francisco A. Muñoz López

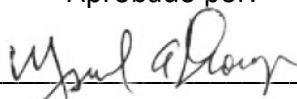
Ha sido aceptado como requisito parcial para el grado de

Maestría En Sistemas De Información

Con Especialidad En Seguridad De Información E Investigación De Fraude

Diciembre, 2019

Aprobado por:



---

Prof. Miguel A. Drouyn Marrero, Ed.D., CISA, CFE

## Tabla de Contenido

<b>Introducción.....</b>	<b>5</b>
<b>Descripción del Caso.....</b>	<b>5</b>
<b>Número del Caso.....</b>	<b>5</b>
<b>Partes del Caso.....</b>	<b>5</b>
<b>Acusados.....</b>	<b>5</b>
<b>Empresas Involucradas.....</b>	<b>5</b>
<b>Investigadores.....</b>	<b>6</b>
<b>Abogados.....</b>	<b>6</b>
<b>Fiscales.....</b>	<b>6</b>
<b>Jueces.....</b>	<b>7</b>
<b>Trasfondo.....</b>	<b>7</b>
<b>Descripción de hechos.....</b>	<b>7</b>
<b>Acusaciones, cargos y penalidades.....</b>	<b>12</b>
<b>Definición de términos.....</b>	<b>13</b>
<b>Revisión de Lectura.....</b>	<b>16</b>
<b>Fraude Involucrados.....</b>	<b>17</b>
<b>Leyes Aplicables.....</b>	<b>18</b>
<b>Casos Relacionados.....</b>	<b>19</b>
<b>Herramientas de Investigación.....</b>	<b>22</b>
<b>Recreación del Esquema de Fraude.....</b>	<b>23</b>
<b>Simulación.....</b>	<b>26</b>
<b>Informe Forense del Caso.....</b>	<b>27</b>
<b>Resumen Ejecutivo.....</b>	<b>27</b>
<b>Objetivo.....</b>	<b>27</b>
<b>Alcance del Trabajo.....</b>	<b>27</b>
<b>Descripción del Caso.....</b>	<b>27</b>

<b>Descripción de los Dispositivos Utilizados.....</b>	<b>28</b>
<b>Resumen de Hallazgos .....</b>	<b>28</b>
<b>Cadena de Custodia.....</b>	<b>30</b>
<b>Procedimiento.....</b>	<b>33</b>
<b>Conclusión del Informe Pericial.....</b>	<b>36</b>
<b>Discusión del Caso.....</b>	<b>37</b>
<b>Informe de Auditoría y Prevención.....</b>	<b>40</b>
<b>Trasfondo, alcance y objetivos.....</b>	<b>40</b>
<b>Hallazgos Detallados y Recomendaciones.....</b>	<b>41</b>
<b>Condición.....</b>	<b>41</b>
<b>Criterio.....</b>	<b>42</b>
<b>Causa.....</b>	<b>43</b>
<b>Efecto.....</b>	<b>44</b>
<b>Conclusión.....</b>	<b>47</b>
<b>Referencias.....</b>	<b>49</b>

## **Introducción**

Este trabajo presenta el caso donde tres miembros de un grupo cibercriminal de escala internacional han sido acusados por atacar sobre 100 compañías estadounidenses. Estas compañías afectadas se encuentran en 47 estados de los Estados Unidos. Se explicará el procesamiento y las leyes que fueron quebrantadas. De igual manera, se presentará, las consecuencias de esto. Por el hecho de que los tres involucrados son juzgados por separado y dos de ellos se encuentra aún en proceso de extradición a Estados Unidos desde España y Polonia, se tomará solo el procesamiento de Fedir Hladyr.

## **Descripción del caso**

### **Número del Caso**

2:17-cr-00276RSM

### **Partes del Caso**

#### **Acusados**

- Fedir Hladyr
- Dmytro Fedorov
- Andrii Kolpakov

#### **Empresas Involucradas**

- Emerald Queen Hotel and Casino, Tacoma, Washington, EEUU.
- Chipotle Mexican Grill, Denver, Colorado, EEUU
- BECU, Tukwila, Washington, EEUU.

- Jason's Deli, Beaumont, Texas, EEUU.
- Red Robin Gourmet Burgers, Seattle, Washinton, EEUU.
- Sonic Drive-in, Shawnee, Oklahoma, EEUU.
- Taco John's, Cheyenne, Wyoming, EEUU.

### **Investigadores**

Equipo de Trabajo Cibernético de Seattle del FBI y la Oficina del Fiscal Federal para el Distrito Oeste de Washington, con la asistencia de la Sección de Delitos Informáticos y Propiedad Intelectual del Departamento de Justicia y la Oficina de Asuntos Internacionales, el National Cyber-Forensics and Training Alliance, numerosas firmas de seguridad informática e instituciones financieras, oficinas del FBI en todo el país y el mundo, así como numerosas agencias internacionales. De igual forma, Anthony Teelucksingh quien es abogado de la División de crímenes cibernéticos del Departamento de Justicia de EEUU (USA vs Fedir Hladyr, 2018).

### **Abogados**

Arkady L. Bukh (abogado de defensa de Fedir Hladyr)

### **Fiscales**

Andrew C. Friedman (Assistant US Attorney)

Francis Franze-Nakamura (Assistant US Attorney)

Steven Masada (Assistant US Attorney)

Anthony Teelucksingh (Trial Attorney)

### **Jueces**

Chief Judge Ricardo S. Martínez, US District Court for the Western of Washington at  
Seattle

### **Trasfondo**

FEDIR OLEKSIYOVYCH HLADYR, también conocido como: Fedor Gladyr, Fedir Oleksiyovych Gladyr, Glayr Fedir Oleksiyovych, Gladyr Fedor Oleksiyovich, Fedor, das, Fyodor, AronaXus era el cabecilla de la organización criminal. Hladyr de 34 años de edad y nacionalidad ucraniana. Era miembro de un grupo sofisticado de piratería internacional para robar registros de tarjetas de crédito y débito se declararía culpable de piratería y cargos de fraude electrónico en Seattle. Este era el administrador de sistemas de FIN7 y mantenía los servidores del grupo. Las actividades de la organización se extendían a Israel, Ucrania y Rusia.

### **Descripción de hechos**

El acusado FEDIR OLEKSIYOVYCH HLADYR, y otros, desconocidos por el Gran Jurado, formaban parte de un criminal cibernético con motivación financiera. La conspiración se conoce como FIN7, el Grupo Carbanak y el Grupo Navigator (aquí denominado FIN7) consiste en un grupo de actores criminales involucrados en una sofisticada campaña de malware dirigida a los sistemas informáticos de las empresas, principalmente en las industrias de restaurantes, juegos y hospitalidad, entre otros.

Fedir Oleksiyovych Hladyr se desempeñó como administrador de sistemas de alto nivel para FIN7 y mantuvo los servidores y los canales de comunicación utilizados por la organización. Por ejemplo, los miembros de FIN 7 solicitaron a Hladyr que les otorgara acceso a los servidores utilizados por FIN7 para facilitar el esquema de malware. También desempeñó un papel de administración en el esquema al delegar tareas y al proporcionar instrucción a otros miembros del esquema.

Los objetivos de la conspiración incluían piratear redes informáticas protegidas utilizando malware diseñado para proporcionar a los conspiradores acceso no autorizado a los sistemas informáticos de las víctimas y el control de ellos. Los objetivos de la conspiración incluían además la vigilancia de las redes informáticas de las víctimas, y la instalación de malware adicional en las redes informáticas de las víctimas con el fin de establecer la persistencia, robar dinero y propiedades, incluidos los datos de seguimiento de la tarjeta de pago (por ejemplo, crédito y débito), información financiera y propietario y no público información. Los objetivos de la conspiración incluyeron además el uso y la venta de datos e información robados para obtener ganancias financieras de diversas maneras, que incluyen, entre otros, el uso de datos de tarjetas de pago robadas para realizar transacciones fraudulentas en los EE. UU. y en países extranjeros.

La manera y los medios utilizados para llevar a cabo la conspiración incluyen lo siguiente:

FIN 7 desarrolló y empleó varios programas maliciosos diseñados para



infiltrarse, comprometerse y obtener el control de los sistemas informáticos de las compañías víctimas que operan en los Estados Unidos y en otros lugares, incluso dentro del Distrito Oeste de Washington. FIN 7 estableció y operó una infraestructura de servidores, ubicados en varios países, a través de los cuales los miembros de FIN 7 coordinaron la actividad para promover el esquema. Esta infraestructura incluía, pero no se limitaba a, el uso de servidores de comando y control, a los que se accedía a través de paneles de control de botnet personalizados, que se comunicaban y controlaban los sistemas informáticos comprometidos de las compañías víctimas.

FIN 7 creó una empresa líder que hace negocios como Combi Security para facilitar el esquema de malware al tratar de hacer que la conducta ilegal del esquema parezca legítima. Combi Security pretendía operar como una empresa de pruebas de penetración de seguridad informática con sede en Moscú, Rusia y Haifa, Israel. Como parte de los anuncios y las páginas de Internet públicas de Combi Security, FIN7 describió a Combi Security como una empresa de pruebas de penetración legítima que se contrató a las empresas con el fin de probar sus sistemas de seguridad informática. Bajo el pretexto de una empresa de seguridad informática legítima, se reclutaron personas con habilidades de programación de computadoras, alegando falsamente que los posibles empleados estarían involucrados en actividades legítimas.

Testeo de redes de computadoras del cliente. La realidad era que Combi Security era una empresa líder que solía contratar e implementar piratas informáticos a los que se les asignaron tareas para promover la conspiración FIN7.

FIN7 seleccionaba víctimas en el Distrito Oeste de Washington y en otros lugares, utilizando técnicas de phishing para distribuir un software malicioso diseñado para obtener acceso no autorizado, tomar el control y eliminar datos de los sistemas informáticos de varias empresas. Las víctimas seleccionadas de FIN7 incluyen más de 120 empresas identificadas, con miles de ubicaciones de operación individuales en todo EE. UU. FIN7 típicamente inició sus ataques al entregar, directamente y a través de intermediarios, un correo electrónico de suplantación de identidad (phishing) con un archivo malicioso adjunto, utilizando cables en comercios interestatales y extranjeros, a un empleado de la empresa víctima afectada. Los archivos maliciosos adjuntos generalmente eran un documento de Microsoft Word (.doc o .docx) o archivo de texto enriquecido (.rtf) con malware incrustado. FIN 7 utilizó una variedad de mecanismos de entrega de malware en sus archivos adjuntos de suplantación de identidad (phishing), incluidos, pero no limitado a: macros de Microsoft Word, objetos maliciosos de vinculación e incrustación de objetos (OLE), scripts maliciosos visuales básicos o JavaScript y archivos de acceso directo incrustados malintencionados (LNK).

En algunos casos, el correo electrónico de phishing o el archivo adjunto contenía un enlace a malware alojado en servidores controlados por FIN7. El correo electrónico de phishing, a través de representaciones falsas, indujeron de manera fraudulenta al empleado de la empresa víctima a abrir el archivo adjunto o hacer clic en el enlace para activar el malware. Por ejemplo, al apuntar a una cadena de hoteles, el supuesto remitente del correo electrónico puede falsamente afirmar que está interesado en hacer una reserva de hotel. A modo de ejemplo adicional, cuando se dirige a una cadena de restaurantes, el supuesto remitente del correo electrónico de suplantación de identidad (phishing) podría afirmar falsamente que está

interesado en realizar un pedido de catering o presentar una queja sobre el servicio de comida anterior en el restaurante.

En ciertos ataques de phishing, FIN7, directamente ya través de intermediarios, enviaron correos electrónicos de suplantación de identidad (phishing) al personal de las compañías víctimas que tuvieron acceso exclusivo a información interna de propiedad privada, pero no limitado a, empleados involucrados en realizar presentaciones ante la Comisión de Bolsa y Valores de Estados Unidos (SEC). Estos correos electrónicos usaban una dirección de correo electrónico que falsificaba una dirección de correo electrónico asociada con el sistema de archivo electrónico de la SEC, e inducía a los destinatarios a activar el malware contenido en los archivos adjuntos de los correos electrónicos.

En muchos de los ataques de FIN7, un miembro de FIN7, o alguien contratado por FIN7 específicamente para tal propósito, también llamaría a la compañía víctima, utilizando cables en el comercio interestatal o extranjero, para legitimar el correo electrónico de phishing y convencer al empleado de la empresa víctima para abrir el documento adjunto utilizando técnicas de ingeniería social. Por ejemplo, cuando se dirige a una cadena de hoteles o una cadena de restaurantes, un conspirador realiza una llamada de seguimiento afirmando falsamente que los detalles de una solicitud de reserva, pedido de catering o queja del cliente se pueden encontrar en el archivo adjunto al correo electrónico entregado anteriormente, para inducir al empleado de la empresa víctima a leer el phishing y desde su correo electrónico, abrir el archivo adjunto y activar el malware.

Si el destinatario activó el archivo adjunto de correo electrónico de suplantación de identidad (phishing) o hizo clic en el enlace, el destinatario activaría el malware sin saberlo, y la computadora en la que se abrió se infectaría y se conectaría a uno o más comandos y controle los servidores controlados por FIN7 para informar los detalles de la computadora recién infectada y descargar malware adicional. La infraestructura de comando y control se basó en varios servidores en varios países, incluidos, entre otros, los Estados Unidos, que generalmente se alquilan con información falsa, como nombres de alias e información ficticia.

FIN 7 típicamente instalaría malware adicional, incluyendo el malware Carbanak, para conectarse a los servidores adicionales de comando y control FIN 7 para establecer el control remoto de la computadora víctima. Una vez que la computadora de la víctima estaba comprometida, FIN 7 incorporaría la máquina comprometida en una red de bots.

FIN7 diseñó y usó un panel de control de botnet personalizado para administrar y emitir comandos a las máquinas comprometidas. Una vez que las computadoras de una compañía de la víctima fueron incorporadas en el botnet y controlado de forma remota por malware, el grupo usó este control remoto y el acceso para, entre otras cosas, instalar y administrar malware adicional, realizar vigilancia, mapear y navegar por la red informática comprometida, comprometer computadoras adicionales, archivos exfiltrados y enviar y recibir datos.

### **Acusaciones, cargos y penalidades**

1. Conspiración para cometer fraude por cable, como se acusa en violación del Título 18, Código de los Estados Unidos, sección 1349

2. Conspiración para cometer piratería informática, como se acusa en el Conde 16, violación del Título 18, Código de los Estados Unidos, sección 371.

### **Definición de términos**

**Hacker** - Según Harvey (1985), profesor de la Universidad de California - Berkley es alguien que vive y respira computadoras, que sabe todo sobre computadoras, que puede hacer que una computadora haga cualquier cosa. Sin embargo, igualmente importante es la actitud del hacker. La programación de computadoras debe ser un pasatiempo, algo hecho por diversión, no por un deber o por el dinero.

**Malware** – CISCO (2019), establece que un malware como un software intrusivo diseñado para dañar y destruir computadoras y sistemas informáticos. El malware es una contracción para el "software malicioso". Ejemplos de malware común incluyen virus, gusanos, virus troyanos, spyware, adware y ransomware.

**IP** - Tech Terms (2016), indica es una dirección única que identifica un dispositivo en Internet o en una red local. Permite que un sistema sea reconocido por otros sistemas conectados a través del protocolo de Internet. Hay dos tipos principales de formatos de dirección IP utilizados hoy: IPv4 e IPv6.

**Servidor** - Un servidor es una computadora diseñada para procesar solicitudes y entregar datos a otra computadora a través de Internet o una red local (USA vs Fedir Hladyr, 2018).

**Carnabak Malware** - Es el nombre dado por los investigadores de seguridad informática a un programa de software malicioso en particular. Carnabak se ha utilizado para acceder de forma remota a las computadoras sin autorización. El malware Carnabak permite que un atacante espíe la computadora de otra persona y controle remotamente la computadora. Carnabak puede grabar videos de la pantalla de la computadora de la víctima y enviar las grabaciones al atacante. También puede permitir que el atacante use la computadora de la víctima para atacar otras computadoras y robar archivos de la computadora de la víctima e instalar otro malware. Todo esto puede hacerse sin el conocimiento o permiso del usuario legítimo (USA vs Fedir Hladyr, 2018).

**Bot** - Una computadora "bot" es una computadora que ha sido infectada con algún tipo de software o código malicioso y luego está sujeta al control de otra persona que no sea el verdadero propietario. El verdadero propietario de la computadora infectada generalmente puede usar la computadora como lo hizo antes de que se infectara, aunque la velocidad o el rendimiento pueden verse comprometidos (USA vs Fedir Hladyr, 2018).

**Botnet** - Una "botnet" es una red de computadoras comprometidas conocidas como "bots" que están bajo el control de un ciberdelincuente o "pastor de bots". Los "bots" son aprovechados por el pastor de bots a través de la instalación subrepticia de malware que proporciona al pastor de bots acceso remoto y control de las computadoras comprometidas. Se puede usar una botnet en masa, de manera coordinada, para entregar una variedad de ataques basados en Internet, incluidos ataques DDoS, ataques de contraseña de fuerza bruta, la transmisión de correos electrónicos no deseados, la transmisión de correos electrónicos de phishing y el

alojamiento de redes de comunicación para cibercriminales (p. ej., actúa como un servidor proxy para las comunicaciones por correo electrónico) (USA vs Fedir Hladyr, 2018).

**Phishing** - Es un esquema criminal en el que los perpetradores usan mensajes de correo electrónico masivos y / o sitios web falsos para engañar a las personas para que proporcionen información como credenciales de red que luego pueden usarse para obtener acceso a los sistemas de la víctima (USA vs Fedir Hladyr, 2018).

**Spear Phishing** - Es una forma específica de phishing dirigida a un individuo, organización o empresa específica. Aunque a menudo intentan robar datos con fines maliciosos, los ciberdelincuentes también pueden usar esquemas de phishing para instalar malware en la computadora de un usuario objetivo (USA vs Fedir Hladyr, 2018).

**Ingeniería Social (Social Engineering)** - Es una habilidad desarrollada con el tiempo por personas que buscan adquirir información protegida a través de la manipulación de las relaciones sociales. Las personas con experiencia en ingeniería social pueden convencer a las personas clave para que divulguen información protegida o accedan a credenciales que el ingeniero social considere valiosas para el logro de sus objetivos (USA vs Fedir Hladyr, 2018).

**Pen Testing** - La prueba de penetración es la práctica de probar un sistema informático, una red o una aplicación informática para encontrar vulnerabilidades que un atacante pueda explotar (USA vs Fedir Hladyr, 2018).

## Revisión de Lectura

### - ¿Qué es un Hacker?

Según Rose (2017) que un pirata informático es una persona que usa la computadora, las redes u otras habilidades para superar un problema técnico. El término pirata informático puede referirse a cualquier persona con habilidades técnicas, pero a menudo se refiere a una persona que usa sus habilidades para obtener acceso no autorizado a sistemas o redes para cometer delitos. Un pirata informático puede, por ejemplo, robar información para herir a las personas a través del robo de identidad, dañar o derribar sistemas y, a menudo, mantener a esos sistemas como rehenes para cobrar un rescate. El término hacker ha sido históricamente divisivo, a veces utilizado como un término de admiración para una persona que exhibe un alto grado de habilidad, así como creatividad en su enfoque de los problemas técnicos. Sin embargo, el término se aplica más comúnmente a un individuo que usa esta habilidad para propósitos ilegales o poco éticos.

### - Efectos de la piratería informática en una empresa

El robo de datos puede ser grave para una organización o un individuo. La pérdida de información comercial para los ladrones puede significar una pérdida de ventaja competitiva para una empresa. También puede traer consecuencias legales, si los datos son información protegida que pertenece a un tercero, como un cliente. Si se roban comunicaciones privadas como mensajes de texto o mensajes de correo electrónico, esto también puede ser bastante embarazoso



para las personas involucradas, si se discutieran temas delicados. Si los datos robados incluyen nombres de usuario y contraseñas adicionales, los datos robados pueden usarse para comprometer computadoras adicionales. Si se roban los datos del banco o de la tarjeta de crédito, eso también se puede usar para robar dinero o realizar compras fraudulentas. Si cree que sus nombres de usuario y contraseñas han sido robados, cambie los nombres de usuario y las contraseñas de inmediato. Además, comuníquese con las instituciones financieras si la información de su cuenta parece haber sido comprometida (Morrow, 2017).

### **Fraudes Involucrados**

- Conspiración

Hubo un acuerdo por parte de un grupo de personas para cometer al menos un delito según lo acusado en la acusación, a saber, Acceso a una computadora protegida para fomentar el fraude. El acusado se convirtió en miembro de la conspiración sabiendo al menos uno de sus objetos y con la intención de ayudar a lograrlo. Uno de los miembros de la conspiración realizó al menos un acto abierto con el propósito de llevar a cabo la conspiración (USA vs Fedir Hladyr, 2018).

- Acceso a una computadora protegida

El demandado accede a sabiendas, sin autorización, a una computadora utilizada en el comercio o comunicación interestatal o extranjera o que se encuentra fuera de los Estados Unidos, pero que la utiliza de una manera que afecta el comercio o la comunicación interestatal o extranjera en los Estados Unidos. Al hacerlo, el acusado

promovió el fraude previsto. El acusado a sabiendas causó la transmisión de un programa, un código o información a una computadora. El acusado perjudica intencionalmente sin autorización la integridad o disponibilidad de datos, un programa, un sistema o información (USA vs Fedir Hladyr, 2018).

### **Leyes Aplicables**

- Título 18, U.S. Code § 1349 Intento y conspiración

Cualquier persona que intente o conspire para cometer un delito en virtud de este capítulo estará sujeta a las mismas sanciones que las prescritas para el delito, cuya comisión fue el objeto del intento o la conspiración (GovInfo, 2014).

- Título 18, U.S. Code, § 371 Conspiración para cometer un delito o defraudar a Estados Unidos

Si dos o más personas conspiran para cometer un delito contra los Estados Unidos, o para defraudar a los Estados Unidos, o cualquier agencia de los mismos de cualquier manera o para cualquier propósito, y una o más de esas personas realizan cualquier acto para hacer el objeto de la conspiración, cada uno será multado bajo este título o encarcelado no más de cinco años, o ambos (GovInfo, 2014).

Sin embargo, si el delito, cuya comisión es el objeto de la conspiración, es solo un delito menor, el castigo por tal conspiración no excederá el castigo máximo previsto para dicho delito menor (GovInfo, 2014).

## Casos Relacionados

### United States v. Justin Tanner Petersen, 98 F.3d 502 (9th Cir. 1996)

El acusado en Estados Unidos v. Petersen, era un hacker experto. Penetró el sistema informático de una agencia nacional de informes de crédito y robó información personal con la cual solía pedir tarjetas de crédito de forma fraudulenta. Luego pirateó la computadora de un prestamista comercial nacional y consiguió que le enviara \$ 150,000 a través de otros dos bancos. Esto va mucho más allá de las habilidades informáticas de un joven inteligente o incluso de muchas personas que se ganan la vida como técnicos informáticos e ingenieros de software. El tribunal de distrito encontró que Petersen tenía "un conocimiento extraordinario de cómo funcionan las computadoras y cómo se almacena la información, cómo se recupera la información y cómo se puede preservar o invadir la seguridad de esos sistemas" e impuso el ajuste de habilidades especiales (USA vs Petersen, 1996).

En CR 92-00575-SVW, Petersen se declaró culpable de todos los cargos de una información de cuatro cargos. El primer cargo acusó a Petersen de conspiración para obtener acceso no autorizado a un sistema informático de interés federal para llevar a cabo un plan para defraudar e interceptar comunicaciones electrónicas y por cable en violación de 18 U.S.C. §§ 371 (USA vs Petersen, 1996).

### United States v. Batti, 631 F.3d 371 (6th Cir. 2011)

Luay Batti trabajó en el departamento de TI de Campbell-Ewald, una empresa de publicidad en Michigan, durante aproximadamente seis años, hasta que fue despedido en

marzo de 2007. Los eventos que llevaron a su terminación comenzaron unos seis meses antes cuando Batti accedió al servidor de la computadora de Campbell-Ewald y copió archivos confidenciales de computadora pertenecientes al CEO de Campbell-Ewald sin autorización. Aunque estos archivos normalmente se almacenaban en la computadora de escritorio del CEO, la compañía los había trasladado al servidor de la compañía mientras se reemplazaba la computadora del CEO. Dentro de estos archivos había "piezas confidenciales de información ... incluyendo compensación ejecutiva, estados financieros de la firma, metas y objetivos para altos ejecutivos de la compañía que reportan al presidente y algunos planes estratégicos". Dist. Connecticut. Dkt. ("Doc.") 35 ("Trial Tr.") En 59.

El registro no revela por qué Batti retuvo esta información durante seis meses, pero, en la noche del 27 de febrero de 2007, fue a la oficina del Vicepresidente y Gerente General de Campbell-Ewald \* 373, Joseph Naporano, para hablar sobre la información. él había obtenido. El aparente propósito de Batti al acercarse a Naporano era simplemente informarle de las debilidades en las barreras de seguridad informática de Campbell-Ewald y quejarse de la gestión del departamento de TI. En esta reunión, Batti también le dio a Naporano una carta en la que Batti expuso sus quejas y un disco de computadora que contenía algunos de los archivos del CEO que Batti había copiado. El disco también contenía imágenes de video que Campbell-Ewald había comprado para su uso en comerciales de televisión para su cliente más grande, General Motors. Poco después, Naporano comenzó a investigar las debilidades de seguridad mencionadas por Batti y, dentro de unos días, Naporano despidió a Batti por ejercer "mal juicio" al acceder y copiar los archivos del CEO. Trial Tr. a los 63.

Aproximadamente seis semanas después, el 18 de abril de 2007, mientras la revisión de seguridad aún estaba en marcha, Naporano se enteró de dos sitios web que contenían información confidencial sobre Campbell-Ewald y GM, junto con correos electrónicos enviados entre funcionarios de estas dos compañías. Estos sitios web estuvieron abiertos al público por un tiempo desconocido, aunque probablemente breve, pero casi inmediatamente después de que Campbell-Ewald los descubrió, quedaron protegidos con contraseña. Muy alarmado por lo que claramente era una violación del sistema de seguridad informática de la compañía, y sin saber exactamente qué tan amplia fue la violación, Naporano se contactó con la policía y una empresa de seguridad de TI, quienes recomendaron que Naporano contactara al FBI. El FBI determinó que Batti había accedido a los archivos confidenciales de Campbell-Ewald no menos de veintiún veces después de su despido, dos veces a través de un servidor de Campbell-Ewald y diecinueve a través de la cuenta de correo electrónico de otro empleado de Campbell-Ewald, Steve Majoros. El FBI realizó una búsqueda en la casa de Batti el 19 de abril de 2007. En una entrevista con el FBI, Batti admitió que había accedido al sistema de Campbell-Ewald a través de su servidor y el correo web de Majoros. En el último punto, Batti admitió que había aprendido el nombre de usuario y la contraseña de Majoros en el transcurso de su empleo con Campbell-Ewald; Aunque Majoros había modificado ligeramente su contraseña después de que Batti fuera despedido, Batti pudo adivinar la nueva contraseña mediante prueba y error. Finalmente, después de esta entrevista, Batti envió dos correos electrónicos al FBI en los que intentó explicar sus acciones.

Además del trabajo realizado por el FBI, la empresa de seguridad informática realizó una investigación sustancial, y Naporano obtuvo asesoramiento legal sobre la violación de seguridad del abogado externo de Campbell-Ewald. El costo total de la investigación de la empresa de seguridad y el asesoramiento del abogado ascendió a \$ 47,565. Además, muchos de los empleados de Campbell-Ewald ayudaron con la investigación. En total, los empleados de Campbell-Ewald pasaron aproximadamente 747 horas lidiando con la violación de seguridad (USA vs .

### **Herramientas de Investigación**

#### FTK

FTK es una plataforma de investigaciones digitales aprobada por los tribunales, que está diseñada para ser veloz, analítica y contar con escalabilidad de clase empresarial. Conocida por su interfaz intuitiva, el análisis de correo electrónico, las vistas personalizadas de datos y su estabilidad, FTK establece el marco para una expansión sin problemas, por lo que su solución de informática forense puede crecer de acuerdo a las necesidades de su organización (Access Data, 2019).

Además, FTK ofrece nuevos módulos de expansión, entregando el primer software de esta industria con capacidad de análisis y con visualización de última generación. Estos módulos se integran con FTK para crear la plataforma de informática forense más completa en el mercado (Access Data, 2019).

#### Sleuth Kit +Autopsy

Es un kit de herramientas forenses digitales de código abierto que se puede utilizar para realizar un análisis en profundidad de varios sistemas de archivos. La autopsia es esencialmente una interfaz gráfica de usuario que se encuentra en la parte superior de The Sleuth Kit. Viene con características como análisis de línea de tiempo, filtrado de hash, análisis de sistema de archivos y búsqueda de palabras clave de fábrica, con la capacidad de agregar otros módulos para una funcionalidad extendida (Autopsy, 2019).

### **Recreación del Esquema de Fraude**

Hdlyr fue contratado para ser el administrador de sistemas de CombiSecurity, aproximadamente el 28 de agosto de 2015. Una de las responsabilidades del Demandado era proporcionar a docenas de miembros de FIN7 acceso a una variedad de servidores de comunicación y servidores de comando y control utilizados por el grupo de piratería. Estos servidores, incluidos JABBER, JIRA, HipChat y servidores de panel de control de botnet personalizados, entre muchos otros. Después de que el acusado se unió a CombiSecurity, rápidamente recibió más y más responsabilidad en el esquema de piratería. Entre otras cosas, fue responsable de agregar información de tarjetas de pago robadas, brindar orientación técnica a los miembros de FIN7, emitir asignaciones para hackers de fin7 y supervisar al equipo de hackers. Rutinariamente transmitía órdenes del liderazgo de primer nivel de FIN7 a otros miembros del grupo (USA vs Hdlyr, 2019).

Desde aproximadamente agosto de 2015 hasta su arresto el 10 de enero de 2018, el Demandado fue miembro de un grupo de piratería motivado financieramente, comúnmente conocido como "FIN7". Comenzando en un momento desconocido, pero a más tardar en agosto

de 2015, y continuando hasta el día del arresto de los Demandados, FIN7 lanzó ataques contra cientos de empresas estadounidenses en un esfuerzo por violar la seguridad de la red de esas víctimas y robar información financiera y no información pública. FIN7 consta de docenas de especialistas en informática con experiencia ubicados en varios países. El acusado a sabiendas e intencionalmente celebró un acuerdo con otros miembros de FIN 7 para obtener acceso no autorizado a computadoras y servidores protegidos de cientos de redes de computadoras protegidas ubicadas en el Distrito Oeste de Washington y en otros lugares de los Estados Unidos, con el objetivo de robar información que luego podría venderse para obtener ganancias financieras. Fin7 usó una compañía de fachada llamada Combi Security para reclutar hackers y proporcionar un velo de legitimidad a la empresa ilegal. Combi Security se presentó como una compañía legítima de seguridad informática que brindaba servicios de pruebas de penetración a una variedad de compañías en todo el mundo. En su sitio web público, Combi Security se presentó como "una de las compañías internacionales líderes en el campo de la seguridad de la información". En realidad, Combi Security no realizó ningún trabajo legítimo y ninguna empresa lo contrató para proporcionar servicios relacionados con la seguridad. FIN7 llevó a cabo sus ataques principalmente mediante el uso de correos electrónicos de phishing y el uso de técnicas de ingeniería social para alentar a los destinatarios de los correos electrónicos de phishing a activar inadvertidamente el malware contenido o adjunto a los correos electrónicos. Una vez activado, el malware conectaría una computadora víctima comprometida a una red de servidores de comando y control ubicados en todo el mundo. A través de su infraestructura de comando y control, FIN7 cargaría malware adicional en las computadoras de las víctimas, realizaría vigilancia y mantendría el control remoto de las computadoras de las víctimas. Entre



otros objetivos, FIN7 buscó ubicar los sistemas POS a través de los cuales podía cargar de forma remota malware en terminales POS que se utilizaron para procesar transacciones de tarjetas de pago en miles de tiendas minoristas y comerciales en todo Estados Unidos. FIN7 luego utilizó el malware para raspar y filtrar la información de la tarjeta de pago. Al hacerlo, FIN7 hizo que se transmitiera en el comercio interestatal y extranjero, numerosas comunicaciones por cable y comandos a terminales POS ubicados en el Distrito Oeste de Washington (USA vs Hdlyr, 2019).

**Figura 1: Simulación del Fraude a Empresas**



**Paso 1:** FIN7 apunta a compañías: particularmente restaurantes de comida rápida y comidas informales, hoteles, casinos y aquellos con una alta frecuencia de transacciones en puntos de venta. FIN7 recopila información para desarrollar mensajes similares a las comunicaciones comerciales rutinarias de la compañía.

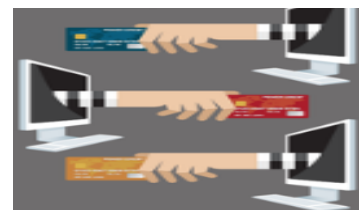


**Paso 2:** Los correos electrónicos de spear phishing se dirigen a los empleados de la empresa víctima, por lo general contactos de cara al público, como los empleados que manejan solicitudes de catering y reservas, y / o en una posición gerencial. FIN7 acompaña los correos electrónicos con llamadas telefónicas para persuadir al empleado de que abra y active el archivo adjunto del correo electrónico, que contiene malware.



**Paso 3:** a) Una vez activado, el malware permite que FIN7 se conecte a la computadora, descargue malware adicional y se mueva a través de la red de la compañía. El malware le permite a FIN7 llevar a cabo la vigilancia de los empleados de la compañía, capturando credenciales para obtener un acceso elevado a la red. b) FIN7 localiza los sistemas de punto de venta que contienen datos de clientes y roba cachés de números de tarjetas de pago.

**Paso 4:** La información de la tarjeta de pago robada vuelve a aparecer en los mercados subterráneos en línea. Los números de tarjeta comprados permiten a los delincuentes hacer cargos no autorizados a los titulares de tarjetas desprevenidos. Los cargos pueden incluir compras minoristas típicas, así como la compra de tarjetas de regalo.



## **Informe Forense del Caso**

### **Resumen Ejecutivo**

En relación al caso en contra del Sr. Fedir Hdlyr, a quien se le acusa de robo y uso indebido de números de tarjetas de crédito o pago, el Lic. Anthony Teelucksingh, abogado litigante de la Sección de Crimen de Computadora y Propiedad Intelectual del Departamento de Justicia de los Estados Unidos de América, ha contratado los servicios de la compañía ABC Corporation para investigar la data almacenada en un dispositivo USB y recuperar cualquier información que involucre al acusado Fedir Hdlyr.

La compañía ABC Corporation es una empresa que se dedica a la consultoría en seguridad cibernética y sus componentes. Con más de 55,000 clientes es la empresa más grande de su tipo en Puerto Rico. Sus operaciones se extienden a Colombia, Ecuador, Panamá y Estados Unidos. La empresa tiene su sede en Bayamón, Puerto Rico.

De acuerdo al Lic. Anthony Teelucksingh, el dispositivo USB contiene la imagen de una computadora que le fue incautada al acusado como parte de las investigaciones que se llevan a cabo tanto internamente como por parte del Departamento de Justicia federal. De encontrarse evidencia contundente en el USB, iría en contra del Sr. Fedir Hdlyr y su posible acusación y sentencia.

### **Objetivo**

El objetivo es obtener la evidencia necesaria para demostrar el robo de tarjetas de crédito y su almacenamiento de forma ilegal. Con este propósito ABC Corporation ha sido contratada para aplicar sus conocimientos de informática forense y lograr demostrar el acceso indebido a la información de los clientes de la compañía.

### **Alcance del Trabajo**

El 27 de abril de 2019 el Lic. Anthony Teelucksingh entrega al Sr. Francisco A Muñoz López un dispositivo USB para ser analizado. En este, se debe encontrar que el sospechoso almacenó los números de tarjeta de crédito de clientes de la compañía para lucro personal y de sus socios en CombiSecutrity. ABC Corp. tiene la encomienda de descubrir, mantener y obtener cualquier evidencia que conduzca a los hechos mencionados para que esta pueda ser enviada al inspector del Departamento del Trabajo. De acuerdo a los estándares forenses el análisis se realiza utilizando las siguientes herramientas:

1. FTK Access Datas Forensic Toolkit

2. FTK Pro Discover Basic
3. FTK Access Data Registry Viewer
4. FTK Imager

Estas herramientas tienen un alto nivel de excelencia y cuenta con el respaldo de la industria de la investigación forense, además, de ser aceptadas por los expertos en el tema. Por, lo tanto se garantiza un alto nivel de ejecución según lo dispone este proceso. ABC Corp, cuample con todas las normas locales y federales en cuanto al manejo, procesamiento y entrega de la evidencia.

Teniendo esto en cuenta, ABC Corp empieza el proceso de adquisición y análisis de la evidencia. Se creará un informe de hallazgos y se notificará al inspector por escrito para que así se pueda tomar la acción que corresponde en estos casos.

### **Descripción del Caso**

1. Número de caso: 2:17-cr-00276-RSM
2. Investigador: Francisco Munoz
3. Cliente: Oficina del Fiscal Federal para el Distrito Oeste de Washington
4. Representante del Cliente: Anthony Teelucksingh quien es abogado de la División de crímenes cibernéticos del Departamento de Justicia de EEUU.

### **Descripción de los Dispositivos Utilizados**

El siguiente listado detalla todos los dispositivos utilizados en el proceso de investigación:

1. HP Touchscreen 15.6 inch HD Notebook (2018 Newest), Latest Intel Core i5-8250U Processor 3.40 GHz, 11GB DDR4, 2TB Hard Drive, Optical Drive, Webcam, Backlit Keyboard, Bluetooth, Windows 10 Home. Esta es donde se encuentran la herramientas utilizadas para este proceso.
2. USB – permite la adquisición de información de un disco sin crear la posibilidad de que se dañe accidentalmente el contenido de la unidad original de donde se extrae la data. Esto es logrado al bloquear cualquier comando de escritura al dispositivo analizado y convirtiéndolo en un dispositivo de solo-lectura.

### **Resumen de Hallazgos**

Este procedimiento de análisis compone la obtención, preservación, compresión y presentación de evidencia digital. Este tipo de evidencia en muchos casos es frágil y el investigador, podría sin intención alguna, alterar o eliminar la información contenida en

cualquiera de los dispositivos que está bajo análisis. Por consiguiente, esta prueba puede ser considerada nula ante un tribunal de justicia.

Para evitar cualquier posible error que conlleve a este suceso ABC Corp emplea el Electronic Data Recovery Model (EDRM) para así obtener una evidencia que sea confiable e íntegra y la misma no pueda ser objetable frente a un juez o jurado.

Se incluye prueba de la evidencia encontrada. El procedimiento de llegar a esta prueba y sus respectivas explicaciones se encuentran más adelante en este informe.

**Figura 2: Listado de las tarjetas de crédito encontradas. Vea que existen cinco tipos de tarjetas de crédito comúnmente utilizadas en la industria de servicios.**

Evidence Items			File Status			File Category		
Evidence Items:	1	KFF Alert Files:	0	Documents:	11			
File Items		Bookmarked Items:	0	Spreadsheets:	1			
Total File Items:	13	Bad Extension:	0	Databases:	0			
Checked Items:	0	Encrypted Files:	0	Graphics:	0			
Unchecked Items:	13	From E-mail:	0	Multimedia:	0			
Flagged Thumbnails:	0	Deleted Files:	0	E-mail Messages:	0			
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	0			
Filtered In:	13	Duplicate Items:	0	Archives:	0			
Filtered Out:	0	OLE Subitems:	0	Folders:	0			
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	0			
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0			
		Data Carved Files:	0	Unknown Type:	1			

	A	B	C	D	E
1	Diners Club	Discover	VISA	MasterCard	American Express
2	30029292957175	6011453429829000	4539458685942560	5207186390871650	377286414106948
3	30244857532293	6011080993767990	4024007107070490	5144311190606050	340898584995910
4	30288325994098	6011227619725300	4556012356161550	5160581145358400	373010029646393
5	30396147925933	6011791507725690	4916781870884610	5358429356107380	341471566084662
6	30128498642837	6011486144619510	4024007180201250	5165287143764020	349302371218579
7	30080996887770	6011731952269550	4539068036509810	5470490033196710	349594858586912
8	30068869607953	6011488146494100	4916810031081340	5202767070498520	379454602034391
9	38268796477130	6011956054523260	4556932298180880	5140395769239290	376011229686053
10	38770575742154	6011555887517240	4916233011908650	5282694741347430	349535596709423
11	38656043606172	6011240879003000	4929184600601030	5104051892578170	377967237874891
12	36423783520093	6011927606089870	4929626999083910	5116809549574580	371357285465451
13	30235430430898	6011556512277030	4929318591860100	5517444938252790	372067851345917
14	36170170641574	6011709949807430	4539972375682710	5128540250501700	378080399200563
15	36140871348266	6011224813697730	4485404538787360	5486494563640470	370366573349955
16	36370659597434	6011234976818160	4556409454476630	5117181746118150	342563232944300
17	30017428987224	6011291216130400	4929934856115890	5585438739523620	379193925139012
18	30223438194146	6011110025266800	4916262892597970	5125094132790170	379976632629196
19	30336513461824	6011120654471010	4716142015234670	5176834564753040	371470086305892
20	30229185268397	6011342771708810	4556298292471460	5232289214468810	341960796104282
21	30336387755970	6011635172306090	4916711828743440	5315728721470830	377341759236691

**Figura 3: Listado de sobre diez mil tarjetas de crédito. En este caso se cuenta el tipo de tarjeta, número, código de seguridad, pin, balance, fecha de expiración, nombre del dueño de la tarjeta, dirección y país.**

AccessData FTK 1.81.6 DEMO VERSION -- C:\ProgramData\AccessData\Forensic Toolkit 1.81.6\DefaultCase\

File Edit View Tools Help

Evidence Items		File Status		File Category	
Evidence Items:	2	KFF Alert Files:	0	Documents:	12
<b>File Items</b>		Bookmarked Items:	0	Spreadsheets:	1
Total File Items:	14	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	0
Unchecked Items:	14	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	0	E-mail Messages:	0
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	0
Filtered In:	14	Duplicate Items:	0	Archives:	0
Filtered Out:	0	OLE Subitems:	0	Folders:	0
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	0
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	1

```

"number": "4438 8852 9037 1952",
"cw": 605,
"pin": 8590,
"balance": "$1587",
"expiration-month": 5,
"expiration-year": 2021
},
"customer": {
"name": "Leslie Warner",
"address": "Eaton Close 3843",
"country": "Netherlands"
}
},
{
"data": {
"card": {
"network": "Maestro",
"number": "6304 1454 7185 8681",
"cw": 467,
"pin": 4774,
"balance": "$11139",
"expiration-month": 9,
"expiration-year": 2027
},
"customer": {
"name": "Christina Cruz",

```

## Cadena de Custodia

Todo proceso comenzado por ABC Corp asegura que se establezcan una cadena de custodia en donde mantenga la integridad de la evidencia. La cadena de custodia presenta el proceso de adquisición, análisis y control de toda evidencia. En el siguiente documento se detalla la cadena de custodia seguida por ABC Corp.

### Primer Evento

- **Descripción del evento:** Evidencia recogida en el Tribunal Federal del Distrito de Puerto Rico. Las oficinas están localizadas en la Avenida Carlos Chardón, Hato Rey, San Juan, Puerto Rico. El Lic. Anthony Teelucksingh entregó la misma al Sr. Francisco Muñoz. La evidencia consiste de un dispositivo USB.
- **Evento verificado por:** Francisco Muñoz y Ricardo Rivera.
- **# de evidencia:** 2:17-cr-00276-RSM

- **Fecha de comienzo:** 27 de abril de 2019
- **Fecha de terminación:** 27 de abril de 2019
- **Lugar de origen:** Tribunal Federal del Distrito de Puerto Rico
- **Destino:** Laboratorio forense – ABC Corp.

#### **Segundo Evento:**

- **Descripción del evento:** Creación de número de caso y asignación de evidencia al mismo.
- **Evento verificado por:** Francisco Muñoz.
- **# de evidencia:** Evidencia E-3256-152 Asignada al caso # 2:17-cr-00276-RSM
- **Fecha de comienzo:** 27 de abril de 2019
- **Fecha de terminación:** 27 de abril de 2019
- **Lugar de origen:** Laboratorio forense – ABC Corp.
- **Destino:** Laboratorio forense – ABC Corp.

#### **Tercer evento:**

- **Descripción del evento:** Proceso de adquisición y análisis de evidencia. Se encontraron dos archivos individuales en el USB. Refiérase a la sección de procedimientos en este reporte para detalles específicos del proceso.
- **Evento verificado por:** Francisco Muñoz.
- **# de evidencia:** Evidencia # E-23-56-86958 asignada al caso #2:17-cr-00276-RSM
- **Fecha de comienzo:** 4 de mayo de 2019
- **Fecha de terminación:** 4 de mayo de 2019
- **Lugar de origen:** Laboratorio forense – ABC Corp.
- **Destino:** Laboratorio forense – ABC Corp.

#### **Cuarto evento:**

- **Descripción del evento:** Entrega de informe de análisis forense al Lic. Anthony Teelucksingh para su evaluación. El informe fue entregado directamente al Lic. Anthony Teelucksingh por parte del investigador a cargo de la evidencia, Francisco Muñoz.
- **Evento verificado por:** Francisco Muñoz y Lic. Anthony Teelucksingh
- **# de evidencia:** Reporte referente a la evidencia # E-3256-152 y E-23-56-86958 – asignada al caso # 2:17-cr-00276-RSM
- **Fecha de comienzo:** 9 de mayo de 2019.
- **Fecha de terminación:** 9 de mayo de 2019.
- **Lugar de origen:** Laboratorio forense – ABC Corp.

- **Destino:** Oficina del Lic. Anthony Teelucksingh.

#### **Quinto evento:**

- **Descripción del evento:** Explicación sobre la información encontrada y su reporte al Lic. Anthony Teelucksingh. El informe fue explicado y aclarado directamente al Lic. Anthony Teelucksingh por parte del investigador a cargo de la evidencia, Francisco Muñoz en el edificio del Tribunal Federal de EEUU en Puerto Rico.
- **Evento verificado por:** Francisco Muñoz y Lic. Anthony Teelucksingh
- **# de evidencia:** Explicación referente a la evidencia  
# E-3256-152 y E-23-56-86958 – asignada al caso # 2:17-cr-00276-RSM
- **Fecha de comienzo:** 11 de mayo de 2019.
- **Fecha de terminación:** 11 de mayo de 2019.
- **Lugar de origen:** Tribunal Federal de EEUU.

#### **Procedimiento**

Luego de culminar el proceso de análisis del contenedor de evidencia - **USB** – y por medio de la herramienta FTK Forensic Toolkit logramos descubrir múltiples archivos en los siguientes formatos:

1. .xlsx
2. .txt

Los archivos analizados se catalogan de dos formas:

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

A continuación, se detallan los archivos encontrados que por la naturaleza de la información contenida se catalogan como evidencia inculpatória con relación al acusado en este caso:



## New Case

**AccessData's  
Forensic Toolkit®-FTK®**  
*The Complete Analysis Tool*

Wizard for Creating a New Case

Investigator Name:

Case Information

Case Number:

Case Name:

Case Path:

Case Folder:

Case Description:

El acusado Fedir Hladyr es sospechoso de poseer números de tarjetas de crédito de forma ilícita. Siendo esto parte de un esquema de fraude a nivel internacional. |

**Figura 4: Se crea la descripción del caso a investigar.**

Evidence File Name	Evidence Path	Display Name	Identification Name/Nu...
CC2.txt	C:\Users\munoz\OneDrive\Documents	CC2	E-23-56-86958
ListofCC.xlsx	C:\Users\munoz\OneDrive\Documents	ListofCC	E-3256-152

**Figura 5: Se añade la evidencia junto a sus números de identificación respectivamente.**

Evidence Items			File Status			File Category		
Evidence Items:	1	KFF Alert Files:	0	Documents:	11			
<b>File Items</b>		Bookmarked Items:	0	Spreadsheets:	1			
Total File Items:	13	Bad Extension:	0	Databases:	0			
Checked Items:	0	Encrypted Files:	0	Graphics:	0			
Unchecked Items:	13	From E-mail:	0	Multimedia:	0			
Flagged Thumbnails:	0	Deleted Files:	0	E-mail Messages:	0			
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	0			
Filtered In:	13	Duplicate Items:	0	Archives:	0			
Filtered Out:	0	OLE Subitems:	0	Folders:	0			
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	0			
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0			
		Data Carved Files:	0	Unknown Type:	1			

	A	B	C	D	E
1	Diners Club	Discover	VISA	MasterCard	American Express
2	30029292957175	6011453429829000	4539458685942560	5207186390871650	377286414106948
3	30244857532293	6011080993767990	4024007107070490	5144311190606050	340898584995910
4	30288325994098	6011227619725300	4556012356161550	5160581145358400	373010029646393
5	30396147925933	6011791507725690	4916781870884610	5358429356107380	341471566084662
6	30128498642837	6011486144619510	4024007180201250	5165287143764020	349302371218579
7	30080996887770	6011731952269550	4539068036509810	5470490033196710	349594858586912
8	30068869607953	6011488146494100	4916810031081340	5202767070498520	379454602034391
9	38268796477130	6011956054523260	4556932298180880	5140395769232990	376011229686053
10	38770575742154	6011555887517240	4916233011908650	5282694741347430	349535596709423
11	38656043606172	6011240879003000	4929184600601030	5104051892578170	377967237874891
12	36423783520093	6011927606089870	4929626999083910	5116809549574580	371357285465451
13	30235430430898	6011556512277030	4929318591860100	5517444938252790	372067851345917
14	36170170641574	6011709949807430	4539972375682710	5128540250501700	378080399200563
15	36140871348266	6011224813697730	4485404538787360	5486494563640470	370366573349955
16	36370659597434	6011234976818160	4556409454476630	5117181746118150	342563232944300
17	30017428987224	6011291216130400	4929934856115890	5585438739523620	379193925139012
18	30223438194146	6011110025266800	4916262892597970	5125094132790170	379976632629196
19	30336513461824	6011120654471010	4716142015234670	5176834564753040	371470086305592
20	30229185268397	6011342771708810	4556298292471460	5232289214468810	341960796104282
21	30336387755970	6011635172306090	4916711828743440	5315728721470830	377341759236691

Figura 6: Este listado se obtuvo desde el dispositivo USB entregado por el personal del Departamento de Justicia de EEUU. Específicamente se encontró en la sección *Spreadsheet* de FTK.

AccessData FTK 1.81.6 DEMO VERSION -- C:\ProgramData\AccessData\Forensic Toolkit 1.81.6\DefaultCase\

Evidence Items			File Status			File Category		
Evidence Items:	2	KFF Alert Files:	0	Documents:	12			
<b>File Items</b>		Bookmarked Items:	0	Spreadsheets:	1			
Total File Items:	14	Bad Extension:	0	Databases:	0			
Checked Items:	0	Encrypted Files:	0	Graphics:	0			
Unchecked Items:	14	From E-mail:	0	Multimedia:	0			
Flagged Thumbnails:	0	Deleted Files:	0	E-mail Messages:	0			
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	0			
Filtered In:	14	Duplicate Items:	0	Archives:	0			
Filtered Out:	0	OLE Subitems:	0	Folders:	0			
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	0			
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0			
		Data Carved Files:	0	Unknown Type:	1			

```

"number": "4438 8852 9037 1952",
"cw": 605,
"pin": 8590,
"balance": "$1587",
"expiration-month": 5,
"expiration-year": 2021
},
"customer": {
"name": "Leslie Warner",
"address": "Eaton Close 3843",
"country": "Netherlands"
}
},
{
"data": {
"card": {
"network": "Maestro",
"number": "6304 1454 7185 8681",
"cw": 467,
"pin": 4774,
"balance": "$11139",
"expiration-month": 9,
"expiration-year": 2027
},
"customer": {
"name": "Christina Cruz",

```

Figura 7: Listado encontrado en el USB en formato XML. Este se encontró en la parte de *Documents*.

volkit 1.81.6\DefaultCase\

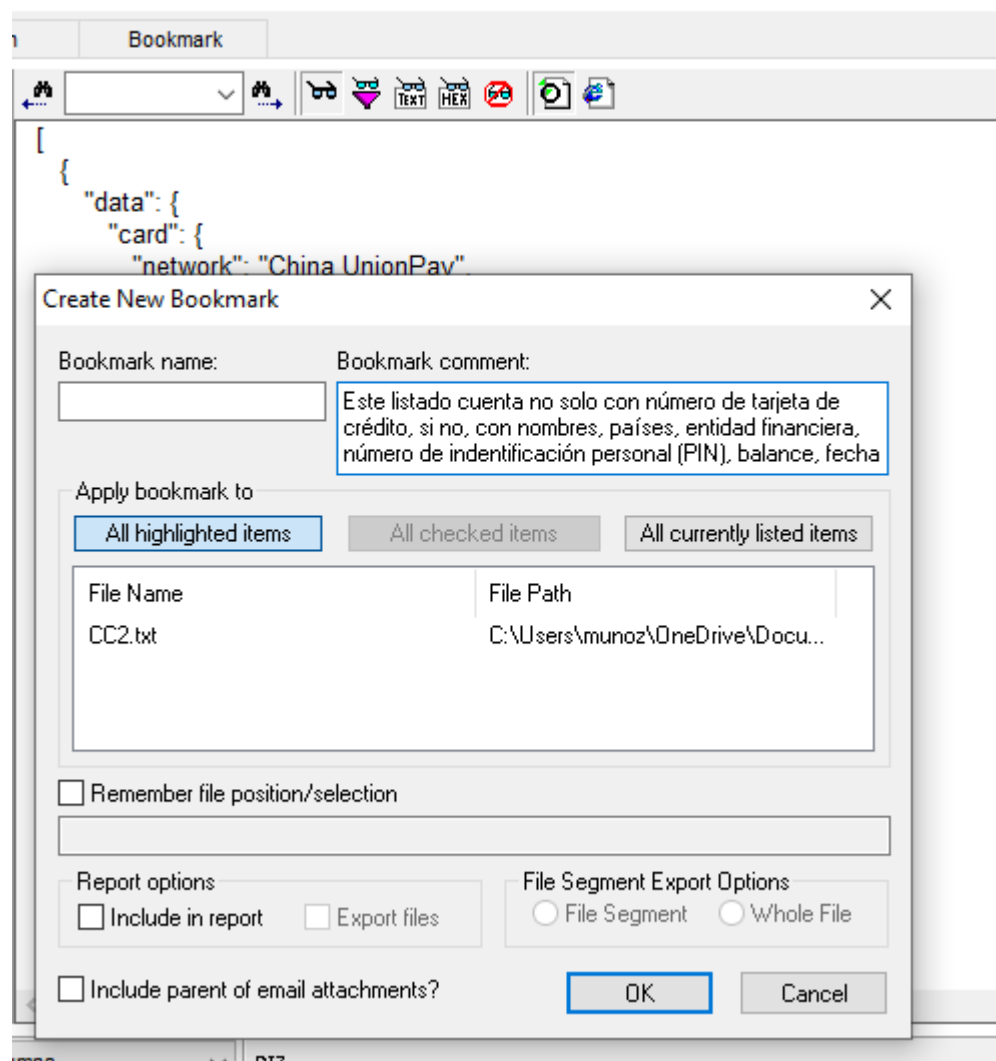


Figura 8: Comentario hecho en la opción de Bookmark para el reporte sobre la anterior figura.

## **Conclusión del Informe Pericial**

Luego de analizar la evidencia, esta presenta ambigüedades. Si bien no se puede eximir al acusado de cualquier mal uso de información de tarjetas de crédito, la evidencia analizada no presenta de forma contundente en contra del Sr. Fedir Hdlyr sea culpable. Si se evidencia sin duda alguna que hubo el acto de almacenar información de tarjetas de crédito que no era suyas. La compañía debe presentar documentación escrita sobre esta política.

Está establecido que el dispositivo no fue alterado por nadie al momento de la entrega. La cadena de custodia claramente establece que ABC Corp recogió el dispositivo la oficina de relaciones laborales bajo la supervisión del Lic. Anthony Teelucksingh y que esta evidencia fue colocada allí por personas autorizadas. Existe copia de la cadena de custodia de dichos agentes que deja establecido que la evidencia fue incautada a Hdlyr en cumplimiento a una orden del Departamento de Justicia de los Estados Unidos de América.

Es por eso por lo que concluimos que toda la evidencia aquí expuesta cumple con todos los estándares de integridad y confiabilidad para ser utilizada en cualquier proceso legal. Además, certificamos que todos los procesos utilizados para la obtención de dicha evidencia cumplen o exceden los parámetros establecidos por el gobierno estatal y federal y las prácticas estándares de la industria forense digital.

## Discusión del Caso

El fraude con tarjetas de pago, posiblemente uno de los enfoques más directos a la delincuencia motivada financieramente, persiste ante los continuos esfuerzos contra el fraude de los reguladores, las instituciones financieras y los minoristas. El cardado, como se le conoce a menudo, es el resultado de actividades coordinadas entre y dentro de las comunidades en todo el mundo del cibercrimen subterráneo, con actividades distribuidas en foros y sitios de la web profunda y oscura (DDW), servicios de chat encriptados y redes sociales abiertas. sitios de medios, donde se sabe que los actores de amenazas comparten videos tutoriales y discuten métodos (Network Security, 2017).

Dado que la actividad de las tarjetas afecta directamente a los consumidores cuyo dinero es robado o cuyos datos están comprometidos, puede tener importantes repercusiones de reputación para las organizaciones que no protegen la información confidencial de la tarjeta. Además, como una amenaza para la seguridad financiera de los ciudadanos, la lucha contra el fraude con tarjetas de pago es a menudo un elemento de acción de alta prioridad para la aplicación de la ley. Como tal, algunas comunidades ilícitas han instituido políticas para prohibir a los usuarios que discuten las tarjetas por temor a que dicha actividad pueda atraer el escrutinio de varias agencias de aplicación de la ley en todo el mundo, incluido el Servicio Secreto de los EE. UU., Que se encarga de abordar los delitos de fraude financiero dirigidos a los ciudadanos y instituciones financieras (Network Security, 2017).

Entre los actores de amenazas, las tarjetas son ampliamente percibidas como dinero fácil, un sentimiento que los analistas de Flashpoint han observado en manuales, tutoriales, sitios web de tarjetas y otros medios ilícitos. Esto se debe en parte a la amplia disponibilidad de

recursos para llevar a cabo actividades de cardado en mercados ilícitos. Algunas de las herramientas y recursos utilizados por los delincuentes incluyen: desnatadores de tarjetas y reflejos para robar datos de tarjetas en terminales de puntos de venta (POS), vertederos que contienen información de tarjetas comprometida junto con PIN y servicios para producir tarjetas físicas clonadas utilizando datos robados. Los delincuentes también pueden producir sus propias tarjetas clonadas comprando software de clonación y equipos de escritura de tarjetas a proveedores en línea (Network Security, 2017).

En términos de inteligencia, los equipos encargados de combatir el fraude con tarjetas de crédito tienen dos requisitos básicos: (a) comprender las tácticas, técnicas y procedimientos en evolución y la dinámica que da forma a la actividad clandestina relacionada con las tarjetas, y (b) la visibilidad continua de si de los datos de su organización ha sido comprometido (Network Security, 2017).

Los correos comprometidos o *phishing* también es otro problema para las compañías. La policía ha vinculado este tipo de correo electrónico comercial con los grupos del crimen organizado internacional, a menudo con sede en Nigeria. La estafa se basa en técnicas sofisticadas de suplantación de identidad (hacer que los correos electrónicos falsos y los documentos comerciales se vean convincentes) y la suplantación de identidad (investigación de una marca para lanzar ataques altamente dirigidos a una población). Los estafadores también pueden usar un malware para infiltrarse en la red informática de una empresa y acceder a intercambios de correo electrónico sobre asuntos financieros. Esta forma de fraude puede dar sus frutos: las víctimas de estafas de correos comprometidos informaron pérdidas de casi \$ 1.3

mil millones al Centro de Quejas de Delitos por Internet (IC3) del FBI en 2018, casi el doble del total del año anterior (Noor, 2019).

A mediados de 2019, los ataques de compromiso de correo electrónico empresarial se dirigían a más de 6,000 empresas por mes, según la empresa de seguridad Symantec. Cualquier empresa u organización, grande o pequeña, puede ser un objetivo. La industria de bienes raíces ha sido particularmente afectada, con los estafadores falsificando correos electrónicos a agentes de bienes raíces, compañías de títulos y otras partes para atrapar pagos de acuerdos de propiedad (Noor, 2019).

Estos esquemas no solo abusan de las empresas: según el FBI, muchas pandillas de compromiso de correos electrónicos comerciales también cometen estafas románticas y de trabajo en el hogar para reclutar "mulas de dinero" involuntarias, manipulando a las víctimas para que abran cuentas bancarias para esconder o lavar el dinero del fraude (Noor, 2019).

El grupo de piratas informáticos, conocido como FIN7 o Carbanak, robó alrededor de 15 millones de registros de tarjetas de crédito y débito y también apuntó a establecimientos en el Distrito de Columbia y en todo el mundo utilizando este tipo de correos electrónicos y fraude a tarjetas de pago (Noor, 2019).

## Informe de Auditoría

### Trasfondo, alcance y objetivos

Tres miembros ucranianos de un grupo sofisticado de piratería internacional que se dirigió a restaurantes, casinos y otros negocios en 47 estados de EE. UU. Para robar registros de tarjetas de crédito y débito han sido arrestados y enfrentan cargos en un tribunal federal en Seattle, dijeron el miércoles funcionarios.

El grupo de piratas informáticos, conocido como FIN7 o Carbanak, robó unos 15 millones de registros de tarjetas de crédito y débito y también se dirigió a establecimientos en EEUU y en todo el mundo.

Estos actores maliciosos son miembros de uno de los grupos de amenazas financieras más prolíficos de esta década, con ataques cuidadosamente diseñados dirigidos a más de 100 organizaciones. Muchos proveedores se refieren a FIN7 como "Grupo Carbanak".

Esta auditoría explora la gama de empresas criminales FIN7, la innovación técnica y el ingenio de ingeniería social que impulsaron su éxito, su aparente uso de una compañía de seguridad como un frente para operaciones criminales y lo que su éxito significa para el panorama de amenazas avanzando.

Este grupo emplea técnicas sofisticadas de ingeniería social y evasión para obtener acceso a los objetivos y mantener continuidad. En todos los casos observados, FIN7 (también conocido como DEV-0099) ha participado en ataques que resultan en ganancias financieras. El grupo ha implementado malware de punto de venta para recopilar información de tarjetas de



pago desde terminales de pago en la tienda. También se han dirigido al personal corporativo que tiene acceso a datos financieros confidenciales, incluidas las personas involucradas en las presentaciones de la SEC. En algunos casos notables, DEV-0099 implementó ransomware y malware de cajeros automáticos en un esfuerzo más directo para obtener ganancias.

### **Hallazgos Detallados y Recomendaciones**

El primer objetivo de la investigación fue identificar el punto de entrada preciso de los atacantes en la red y el método de compromiso inicial ejercido. Esto fue enfocado específicamente en un hotel afectado.

### **Condición**

Los numerosos trabajos realizadas por nuestro equipo identificaron un evento común al comienzo de la línea de tiempo de estos ataques: que uno o más empleados habían recibido lo que parecía ser, a primera vista, un correo electrónico de phishing dirigido con un archivo adjunto de documento de Word potencialmente malicioso.

Si bien el contenido del mensaje parece ser legítimo y está relacionado con los servicios de la organización (sector de la hospitalidad), el correo electrónico contenía un archivo adjunto de documento de Microsoft Word (.docx), 1-list.docx es el nombre de el documento adjunto. Los autores del malware llamaron a la víctima directamente por teléfono y pidieron que se abriera el archivo adjunto para garantizar la infección, ya que la configuración predeterminada en Microsoft Word evita la ejecución de cualquier código macro. Este fue el elemento de

ingeniería social de ataque utilizado para convencer al usuario de ejecutar la macro haciendo doble clic en una imagen que se muestra dentro del documento abierto.

Un examen detallado del documento adjunto de Word demuestra que este fue el vector utilizado por los atacantes para ingresar a la red de la organización objetivo. El archivo 1-list.docx parece ser un malware habilitado para macros, diseñado para eliminar y ejecutar código malicioso en el sistema de destino.

### **Criterio**

La auditoría se realizó en completa normalidad y se contó con la colaboración y acompañamiento de los funcionarios, además se resalta que el sistema de información está en continua renovación y se han implementado nuevas características que benefician a la empresa. Los correos electrónicos de suplantación de identidad pueden parecerse a cualquier otro mensaje molesto de un banco o empresa, pero si ha sido víctima de un ataque de suplantación de identidad, sabe que estos mensajes son mucho más que eso. Por lo tanto, las empresas a menudo les dicen a los empleados que no hagan clic en enlaces o abran archivos adjuntos en correos electrónicos sospechosos.

El hotel cuenta con técnicas anti-phishing para evitar filtraciones de información confidencial. Las sesiones de capacitación regulares son más efectivas que una sola sesión. Estas son algunas de las principales normas implementadas por la compañía matriz del hotel.

- Nunca proporcione información personal cuando se le solicite por correo electrónico:

la mayoría de las compañías legítimas nunca le pedirán que proporcione información confidencial como números de cuenta, contraseñas o datos personales por correo electrónico.

- Tenga cuidado con los errores ortográficos y gramaticales:  
las marcas auténticas toman en serio su copia de la web y del correo electrónico y no publicarán mensajes plagados de errores. Preste especial atención al nombre y al logotipo de la empresa.
- Cuidado con el lenguaje amenazante o imperativo:  
los phishers a menudo usan tácticas de miedo para que los clientes actúen de inmediato por temor a que se suspenda su cuenta.
- Informe los correos electrónicos sospechosos lo antes posible:  
lleve el correo electrónico a un supervisor si tiene alguna duda, y no haga clic en ningún enlace o archivo adjunto si no está seguro de si es auténtico.

## **Causa**

La cultura de prevención comienza en la alta gerencia. La ciberseguridad debe ser tomada en serio por el liderazgo. Esto ayuda a los gerentes a comprender cómo su falta de atención tiene un efecto directo en la postura de seguridad de la empresa (no faltan informes que describen el costo financiero real de los incidentes de ciberseguridad). El personal ejecutivo y de alto nivel debe comprender qué tan grande es la amenaza de la seguridad cibernética para su organización.

La gerencia no proveyó una imagen de las posibles consecuencias si la cultura y, por lo tanto, el comportamiento general no cambiaba. El tema de la seguridad cibernética no estuvo en la agenda de la alta gerencia para que pueda descubrir cómo su cultura, políticas y prácticas deben cambiar para abordar la amenaza de manera efectiva.

De igual forma, la gerencia no hizo capacitaciones continuas ni exámenes sorpresa a sus empleados. La empresa no encontró formas novedosas para recompensar a sus empleados que hubiera pasado satisfactoriamente las pruebas sobre ciberseguridad.

Por otro lado, el hotel no supo exponer satisfactoriamente las expectativas sobre seguridad cibernética. El manual del empleado las responsabilidades de estos sobre la seguridad informática. Ni tampoco las consecuencias a nivel de recursos humanos que podrían enfrentar.

### **Efecto**

Durante las investigaciones de varios eventos maliciosos, algunas de las pruebas ejecutables después de ser descargados por su proceso principal se escribieron directamente en la memoria y luego se inyectaron en otros procesos como archivos DLL y se eliminaron después de realizar su función. Del mismo modo, el uso extendido de los comandos de PowerShell brinda la ventaja a los adversarios de "malware sin disco", también conocido como "malware residente en memoria", escondido detrás del proceso de su host de secuencias de comandos. Además, la práctica de utilizar scripts que son flexibles por naturaleza es otra gran ventaja para los atacantes que les permite modificar su código sin esfuerzo. De igual manera, el uso de tantos tipos diferentes de software malicioso indica fuertemente que varias entidades

están cooperando y comunicándose en los mercados subterráneos para intercambiar herramientas y técnicas. También es posible que algunas de las etapas del ataque hayan sido realizadas por diferentes grupos maliciosos de personas y luego otros grupos hayan continuado. El uso de servicios como Google Docs para hacer un seguimiento de las víctimas y difundir archivos maliciosos se convierte en un gran desafío para los defensores porque de esta manera es muy difícil distinguir entre los buenos y los malos que usan estos servicios populares de nube pública.

Finalmente, las características de ataque de esta familia de malware comparten varios rasgos comunes con la campaña Carbanak original, bien entendida, que se ha atribuido positivamente a la red de ciberdelincuencia financiera. De lo único de lo que podemos estar seguros es de que los atacantes no dejarán de buscar formas nuevas e innovadoras de infectar los entornos corporativos y manipular los servicios públicos, que el público considera leales y confiables.

Se recomienda encarecidamente que las organizaciones de las industrias minorista, de comercio electrónico y hotelería implementen contramedidas estratégicas de inmediato. Realice una evaluación de compromiso exhaustiva de manera proactiva en lugar de esperar los primeros signos de ataque. Realice una búsqueda exhaustiva de amenazas, utilizando la información de esta auditoría de amenazas, en toda la red, incluidos servidores y puntos finales, para identificar cualquier signo de actividad maliciosa. Finalmente, evalúe la capacidad actual de respuesta a incidentes para identificar brechas que afectan la capacidad de respuesta de su organización. Ninguna organización puede brindar protección contra todos los ataques, pero su capacidad para interrumpir efectivamente un ataque y responder de manera rápida y

efectiva tendrá un impacto a largo plazo en su capacidad de supervivencia frente a ataques avanzados.

## Conclusión

Fin7/Carbanak y sus componentes se benefician enormemente de los sistemas no protegidos correctamente en entornos corporativos. De este modo, utilizaban campañas efectivas de spearphishing e ingeniería social junto con los conocidos exploits de MS Office generados por el marco.

Los documentos de phishing FIN7 pueden parecer básicos, pero cuando se combinan con su amplia ingeniería social y concentrados en objetivos específicos, fueron bastante exitosos. Al igual que con su compañía falsa, "Combi Security", la cual lograba esconder las verdaderas intenciones de estos criminales.

En términos de limitar el delito cibernético, tanto la policía como los representantes de tarjetas de crédito hacen las mismas recomendaciones: vigile todas sus transacciones con tarjeta de crédito, informe cualquier sospecha a su compañía de tarjeta de crédito y no abra descargas sospechosas o inesperadas y archivos adjuntos de correo electrónico.

El riesgo cibernético es una prioridad que va en aumento en las organizaciones, ya que el uso de la tecnología en los negocios aumenta y el entorno de amenazas se vuelve más complejo. Es hora de que las organizaciones adopten un enfoque más integral para la resiliencia cibernética, que involucra al equipo ejecutivo completo y abarca la prevención, respuesta, mitigación y transferencia de riesgos. Esto incluye que las compañías deben asegurarse de que estén actualizados con las últimas tecnologías de seguridad en tarjetas de pago y puntos de venta. De igual forma, deben estar más vigilantes de la actividad en las tiendas que aceptan estas tarjetas para identificar y mitigar rápidamente las infracciones y las descargas de tarjetas.

La seguridad debe ocuparse de los problemas que realmente enfrenta la empresa; prevenir el phishing no habría detenido los recientes ataques. Suponiendo que la suplantación de identidad es una preocupación, cuando sea posible hacerlo con la precisión adecuada, los correos electrónicos de suplantación de identidad deben bloquearse. Algunos pasarán, pero con sistemas bien diseñados y rápidamente *'parcheados'*, el daño puede ser limitado. Se debe invertir en programas que creen credenciales de autenticación al phishing. Lo que significaría que las contraseñas robadas no tienen ningún valor. Finalmente, si el malware llega a las computadoras de la compañía, este limitará el daño, ya que el monitoreo efectivo facilita la detección y las buenas copias de seguridad permiten una recuperación rápida.



## Referencias

Access Data. (2019, February 9). Retrieved November 12, 2019, desde

<https://accessdata.com/products-services/forensic-toolkit-ftk>.

Autopsy Digital Forensics. (2019, August 12). Retrieved November 12, 2019, desde

<https://www.autopsy.com/about/>.

CISCO, (2019, octubre 29). What is Malware? - Definition and Examples. Recuperado en noviembre 5, 2019, desde <https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html>.

Clark, V. (2018). Document: Justice Department Unseals the Indictments of Three Members of International Cybercrime Group "Fin7". LAWFARE, . Retrieved , from

<https://www.lawfareblog.com/document-justice-department-unseals-indictments-three-members-international-cybercrime-group-fin7>

Clark, V. (2018). Document: Justice Department Unseals the Indictments of Three Members of International Cybercrime Group "Fin7". LAWFARE, . Recuperado , desde

<https://www.lawfareblog.com/document-justice-department-unseals-indictments-three-members-international-cybercrime-group-fin7>

GovInfo (2011). 18 U.S.C. 371 - Conspiracy to commit offense or to defraud United States.

Retrieved November 12, 2019, from <https://www.govinfo.gov/app/details/USCODE-2014-title18/USCODE-2014-title18-partI-chap63-sec1349/summary>.

GovInfo (2014). 18 U.S.C. 1349 - Attempt and conspiracy. Retrieved November 12, 2019, from <https://www.govinfo.gov/app/details/USCODE-2014-title18/USCODE-2014-title18-partI-chap63-sec1349/summary>.

Harvey, B. (1985). What is a Hacker? Retrieved October 31, 2019, from <https://people.eecs.berkeley.edu/~bh/hacker.html>.

Introducing Basic Network Concepts. (2014). Retrieved November 1, 2019, from [https://www3.nd.edu/~cpoellab/teaching/cse40814\\_fall14/networks.pdf](https://www3.nd.edu/~cpoellab/teaching/cse40814_fall14/networks.pdf).

Komo News (2019). International hacker pleads guilty in Seattle, faces up to 25 years in prison. (2019, September 12). Retrieved November 12, 2019, from <https://komonews.com/news/local/international-hacker-pleads-guilty-in-seattle-faces-up-to-25-years-in-prison>.

Morrow, Bill . (2012) "BYOD security challenges: control and protect your most sensitive data." Network Security. 2012.12 (2012): 5-8. Web. [https://doi.org/10.1016/S1353-4858\(12\)70111-3](https://doi.org/10.1016/S1353-4858(12)70111-3).

Network Security (2017). In brief. Network Security, 2017,(11), 3.  
doi:[https://doi.org/10.1016/S1353-4858\(17\)30089-2](https://doi.org/10.1016/S1353-4858(17)30089-2)

Noor, U., Anwar, Z., Amjad, T., & Raymond Choo, K. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Generation Computer Systems, 19, 227-242. doi:<https://doi.org/10.1016/j.future.2019.02.013>

Revista Seguridad - UNAM (2018). CÓDIGOS MALICIOSOS. (31). Recuperado, desde <https://revista.seguridad.unam.mx/numero-01/c%C3%B3digos-maliciosos>

Rouse, M. (2017, August ). Information Security information, news and tips - SearchSecurity. What is hacker? - Definition from WhatIs.com. Retrieved November 20, 2019, from <http://searchsecurity.techtarget.com/definition/hacker>

Semana (2014) ¿Qué es un Malware y cómo se puede prevenir? Recuperado, desde <https://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913-3>

Tech Terms (2016, septiembre 21). IP Address. Recuperado noviembre 11, 2019, desde [https://techterms.com/definition/ip\\_address](https://techterms.com/definition/ip_address).

U.S. Code › Title 18 › Part I › Chapter 47 › § 1030. Legal Information Institute - Cornell University, . Recuperado , desde <https://www.law.cornell.edu/uscode/text/18/1030>

United States Department of Justice. (2018). Three Members of Notorious International Cybercrime Group “Fin7” In Custody for Role in Attacking Over 100 U.S. companies. Justice News - US Department of Justice , . Retrieved , desde <https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100>

United States v. Batti, (6th Cir. 2011) Recuperado 13 de noviembre de 2012, desde <http://www.opn.ca6.uscourts.gov/opinions.pdf/11a0014p-06.pdf>

United States v. Justin Tanner Petersen, 98 F.3d 502 (9th Cir. 1996)