

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

PHISHING:
**UNA PLATAFORMA SENCILLA PARA EL CIBERATAQUE UTILIZANDO LA
INGENIERIA SOCIAL**

Caso: United States of America Vs. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park”

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN CON
ESPECIALIDAD EN SEGURIDAD DE INFORMACIÓN E INVESTIGACIÓN DE
FRAUDE DIGITAL.

MARZO, 2020

PREPARADO POR
NOEMÍ D. CABA CALDERÓN

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

PHISHING:
**UNA PLATAFORMA SENCILLA PARA EL CIBERATAQUE UTILIZANDO LA
INGENIERIA SOCIAL**

Caso: United States of America Vs. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park”

Preparado por
Noemí D. Caba Calderón

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

Marzo, 2020

Aprobado por:



Dr. Miguel A. Drouyn Marrero, Profesor

Dedicatoria

Dedico esta tesis a una mujer excepcional. Una mujer que por más que los tiempos se pusieron difíciles no desmayó. A esa mujer valiente, que aceptó un reto académico para complementar su desempeño profesional siendo este uno fuerte, ya que venía aislado de su conocimiento y formación primaria. Sí, se la dedico por sus horas de trabajo, por su inalcanzable lucha contra ella misma, por vencer el sueño en las madrugadas, por trabajar duro para el sustento de su familia y el propio y, aun así, no dejar a un lado sus estudios. Se la dedico, porque ella misma merece ser reconocida por ella. Ser reconocida por lo imparable que es y por tener sed y hambre de adquisición. Pero esa mujer tiene motivos que cada día al llegar a su hogar le brinda su apoyo para no desmayar. Cuenta con dos ángeles que Dios le envió para demostrarle su amor infinito, para apoyarla y que le dieran respuestas rápidas a la hora de la desesperación, del cansancio y de esa voz en el interior que le decía “estas cansada, renuncia o déjalo para luego”. Uno de esos ángeles también se involucró en la maestría como si fuera suya, apoyándola en todo el sentido de la palabra. Esto también se lo dedico a esos dos ángeles maravillosos que siempre están conmigo.

Esa mujer tiene apenas 24 años. No sé qué le espere en la vida después de esto. Pero lo que sí sé, es que a donde quiera que valla seguirá siendo imparable aun cuando tenga de frente el mayor reto de su vida. Se la dedico a esa mujer por lo mucho que ha sufrido en esta vida y por qué se merece dedicarse algo ella misma.

Noemí D. Caba Calderón

Tabla de Contenido

SECCIÓN I. INTRODUCCIÓN Y TRASFONDO	8
Introducción.....	8
Descripción del caso.....	9
Partes del caso	9
Trasfondo	10
Descripción de hechos	11
Eventos.....	12
Cargos penales	14
Definiciones de términos	15
SECCIÓN II: REVISIÓN DE LITERATURA.....	19
Introducción.....	19
Fraudes Involucrados	19
Estadísticas.....	21
Leyes aplicables.....	23
Casos relacionados.....	24
SECCIÓN III: SIMULACIÓN DEL CASO	28
Simulación de Fraude.....	30
SECCIÓN IV: INFORME FORENSE DEL CASO	31
Resumen Ejecutivo.....	31
Objetivo.....	31
Alcance del trabajo	32
Datos del caso	32
Descripción de los dispositivos utilizados	32
Resumen de hallazgos.....	34
Cadena de custodia.....	40
Procedimiento.....	42
Conclusión.....	48
SECCION V: DISCUSIÓN DEL CASO	49
SECCIÓN VI. INFORME DE AUDITORÍA Y PREVENCIÓN	50
Trasfondo, alcance y objetivos	50
Hallazgos detallados y recomendaciones	50

SECCIÓN VII. CONCLUSIÓN	52
SECCIÓN VIII. REFERENCIAS	53

Tabla de Figuras

Figura 1 Ficha federal donde identifica al Sr. Park Jin Hyok como una persona de interés. 12

Figura 2 Presenta una página web que aparenta ser legítima, donde se descargan películas gratuitas, que aún están en el cine o no han sido estrenadas por las casas productoras. 21

Figura 3: Gráfica sobre los países que han sido fuentes de SPAM en el pasado 2019. 22

Figura 4: Estadística en porcentaje de cómo son presentados los correos electrónicos falsos. 23

Figura 5: Diagrama que relaciona a Park Jin Hyok con sus víctimas. 29

Figura 6: Diagrama que simula el proceso del delito. 30

Figura 7: Entrega de evidencia del Disco duro GLYPH Blackbox Pro. 33

Figura 8: Intento de autenticación fallido. 34

Figura 9: Intentos de acceso a DESKTOP-2QEUG3J perteneciente a empleado de SPE. 34

Figura 10: Actividad de acceso a correos electrónicos. 35

Figura 11: Correo electrónico amenazante por parte del acusado. 35

Figura 12: Correo electrónico amenazante enviado a empleado de Sony. 36

Figura 13: Correo electrónico amenazante. 36

Figura 14: Se identifica correo enviado a empleado de Sony donde se presenta el mismo apellido del acusado. 37

Figura 15: Currículo que involucra a Park con los hechos contra SPE. 38

Figura 16: Reporte sobre actividad en correos electrónicos. 39

Figura 17: Acceso a página de internet “PASTEBIN”. 39

Figura 18: Plataforma de OSForensics. 43

Figura 19: Extracción de información para análisis. 44

Figura 20: Iniciando análisis y creando expediente. 44

Figura 21: Organización de expediente por categorías. 45

Figura 22: Correo electrónico amenazante por parte del acusado. 46

Figura 23: Correo electrónico amenazante por parte del acusado. 46

Figura 24: Correo electrónico amenazante a empleado de Sony. 47

Figura 25: Correo electrónico enviado por “Kim Jin Woo”. 47

SECCIÓN I: INTRODUCCIÓN Y TRASFONDO

Introducción

A través del tiempo se ha demostrado las incalculables ventajas que tiene la tecnología. Los sistemas computarizados ofrecen oportunidades nuevas de aprendizaje e innovación, pero también hay quienes han creado la posibilidad de cometer delitos informáticos rompiendo cualquier precedente en formas no tradicionales. A esto nos referimos, a que cuando se comete un crimen de cualquier clase requiere planificación, lógicas y autocontrol. En ocasiones se cuestiona si el comportamiento criminal del ser humano va dirigido o impulsado por una conducta que no es racional, donde la maldad abarca la adversidad. Por tanto, podemos deducir que estos eventos delictivos que se concentran en la tecnología requieren de una mente criminal estable, de tiempo y de una buena planificación.

Hoy en día la exposición ante estas amenazas cibernéticas ha sido incalculable, ya que toda persona a través de cualquier aparato inteligente estará expuesta. A través de los años la tecnología ha evolucionado y su auge se ha incrementado por las competencias entre compañías y diseños. Esto, agregando valor al cálculo económico, pero ¿no será que la tecnología realmente nos está pasando factura? Son cuestionamientos que pretendo investigar directa o indirectamente en la ejecución de este caso.

Seleccioné el caso a discutir a continuación porque me parece interesante, maquiavélico y sorprendente conocer todo lo que puede hacer una persona con acceso a internet y un dispositivo.

Entiendo que todas las agencias de estado, el departamento de Seguridad Nacional, los bancos y hasta las agencias de crédito, deberían estar enterados de estos tipos de casos que ponen a las compañías en la línea fina de la desconfianza, la vulnerabilidad y robo de información.

Descripción del caso

Caso: United States of America Vs. Park Jin Hyok, also known as (“aka”) “Jin Hyok Park”

Número de caso: MJ 18-1479

Partes del caso

Acusado:

1. Park Jin Hyok

Entidades involucradas:

1. Lazarus Group
2. Expo Joint Venture

Víctimas:

1. Sony Pictures Entertainment
2. Banco Bangladesh
3. Banco de la reserva federal de New York
4. Industrias de monedas virtuales
5. Servicios públicos
6. Facultades Universitarias
7. Empresas de tecnología
8. Contratistas de la defensa de los Estados Unidos: Lockheed Martin

Investigadores:

1. Nathan P. Shields, agente especial de la Oficina Federal de Investigación (FBI)

Abogados:

1. Christopher A. Wray, abogado y director del FBI.

Fiscales:

1. John C. Demers, fiscal general adjunto de Seguridad Nacional
2. Tracy Wilkison, primer fiscal general adjunto de los EU para el distrito de California

Juez:

1. Hon. Rozella A. Oliver, Jueza del magistrado de los Estados Unidos.

Trasfondo

El acusado se llama Park Jin Hyok, nació en Corea del Norte el 4 de febrero de 1990. Curso estudios en la Universidad Tecnológica Kim Chaek en Pionyang, Corea del Norte. Se destacó siendo programador de computadoras, trabajando más de una década para la compañía Chosun Expo Joint Venture, de inteligencia militar.

Según la acusación del Departamento de Justicia (2018), alega que Park era miembro de un equipo de piratería patrocinado por el gobierno asiático, conocido por el sector privado como el "Grupo Lazarus", y trabajó para una empresa del frente del gobierno de Corea del Norte, Chosun Expo Joint Venture (a / k / a Korea Expo Joint Venture o "KEJV"), para apoyar las acciones cibernéticas maliciosas del gobierno de la RPDC. Las actividades maliciosas de conspiración incluyen la creación del *malware* utilizado en el ataque global de *ransomware* WannaCry 2.0 de 2017; el robo de \$ 81 millones en 2016 del Banco de Bangladesh; el ataque de 2014 contra Sony Pictures Entertainment (SPE); y numerosos otros ataques o intrusiones en las

industrias de entretenimiento, servicios financieros, defensa, tecnología, moneda virtual, academias y servicios públicos.

Descripción de hechos

Según la declaración del Departamento de Justicia (2018), en noviembre de 2014 se lanzó un ataque destructivo contra Sony Pictures Entertainment (SPE), en represalia por la película "The Interview", una comedia absurda que describió el asesinato del líder de la RPDC. Los conspiradores obtuvieron acceso a la red de SPE enviando *malware* a los empleados de SPE y luego robaron datos confidenciales, amenazaron a los ejecutivos y empleados de SPE y dañaron miles de computadoras. Casi al mismo tiempo, el grupo envió mensajes de pesca submarina a otras víctimas en la industria del entretenimiento, incluida una cadena de cines y una compañía del Reino Unido que estaba produciendo una serie de ficción que involucraba a un científico nuclear británico hecho prisionero en la RPDC.

El ataque fue tan masivo que logró la intromisión a la base de datos, robando la identidad de los empleados de SPE a través de *phishing* y programas malignos. Los programas los enviaba vía correo electrónicos a empleados de Sony Pictures Entertainment, si estos eran abiertos les daba acceso de forma automática a Jin Hyok. Una vez dentro de la red de SPE, los sujetos robaron películas, credenciales, información personal de actores y otras informaciones confidenciales, y luego enviaba virus que dejaban las computadoras inoperantes. Los programas malignos enviados contenían *scripts* diseñados para atacar computadoras que ejecutan sistemas operativos Unix o Linux. La denuncia penal de 179 páginas del Departamento de Justicia (2018), afirma que Park era parte de este equipo de piratas informáticos que ha intentado irrumpir en las redes de negocios estadounidenses en un sin número de ocasiones.

El acusado Park Jin Hyok, aún no ha sido atrapado por las autoridades estadounidense. Aun cuando existen confidencias que podrían dar con su paradero, se desconoce con exactitud su ubicación. Se entiende, que su alianza con el gobierno coreano ha sido un factor dominante para que en efecto esto no ocurra. La corte de los Estados Unidos ha emitido sentencias y órdenes de arresto en ausencia contra Park.



Figura 1: Ficha federal donde identifica al Sr. Park Jin Hyok como una persona de interés.

Eventos

1. El 25 de mayo de 2015, un pirata logro acceso a un servidor *web* de Sony por la dirección IP de Corea del Norte # 2, se usó la cuenta de correo electrónico amazonriver1990@gmail.com. Ese usuario se descubrió que también se realizó sustanciales investigaciones en línea sobre temas relacionados con la piratería entre el 19 de mayo de 2015 y 10 de septiembre de 2015, incluidos los relacionados con CVE, software, *code* y métodos de ocultar la dirección IP.

2. El 9 de septiembre de 2014, desde un IP dirección ubicado en los Estados Unidos intentaron realizar una conexión.
3. El 22 de septiembre de 2014 los registros revelaron que la dirección IP de Sony, fue utilizada por un sujeto para explorar un sitio web en distintos momentos.
4. En noviembre de 2014, SPE supo que los ciber atacantes habían ganado el acceso no autorizado a la red informática.
5. El viernes 21 de noviembre de 2014, un sujeto con el nombre "Frank David "envió un correo electrónico a los empleados de alto rango de SPE. El asunto del correo electrónico era "Aviso para Sony Pictures Entertainment Inc." y el cuerpo del correo electrónico declaró lo siguiente: "Tenemos grandes daños por parte de Sony Pictures. Son compensaciones monetarias que queremos. Paga el daño, o Sony Pictures será bombardeado en su conjunto".
6. El 21 de noviembre de 2014, el mismo día en que se envió el correo electrónico, desde una dirección IP controlando el DDNS, se descubrió que se utilizó en adición el servicio de *proxy*.
7. El 24 de noviembre de 2014, el FBI investigó que solo a algunos empleados de Sony les llegó un mensaje por correo electrónico que contenía una supuesta demanda de rescate.
8. El 24 de noviembre de 2014, aproximadamente 21 cuentas de Twitter fueron registrados y utilizados por SPE, se vieron comprometidos; Se descubrieron mensajes enviados donde algunos contenidos en texto eran "Hackeado por #GOP" y "Ustedes, los delincuentes. . . Seguramente irá al infierno. Nadie puede ayudarte ".
9. El 26 de noviembre de 2014, un sujeto envió un correo electrónico de seguimiento con un asunto que leía "LE CASTIGAREMOS por completo". Esto a causa de que Sony

rechazara una demanda. También se recibió otro mensaje que leía “Sony Pictures llegará a saber cuál es el costo de su decisión”, “haremos que Sony Pictures se elimine de la lista de Hollywood, seguramente colapsarás. ¡Maldita sea la cruel e imprudente Sony Pictures!”

10. El 1 de diciembre de 2014, la página de Facebook afirmó tener una suscripción de "Sitio oficial de TheGuardianes de la paz (#GOP) ". La página contenía una imagen similar a las que apareció en algunas de las cuentas comprometidas de SPE en Twitter discutidas anteriormente.
11. El 5 de diciembre de 2014, un sujeto envió un cuarto correo electrónico a numerosos SPE empleados que declararon: “Soy el jefe del Partido Republicano que te hizo preocuparte”.
12. El 11 de diciembre de 2014, se robaron datos nuevos que fueron difundido por los sujetos el 17 de diciembre de 2014.
13. El 16 de diciembre de 2014, un sujeto utilizó públicamente el sitio web Pastebinpublicar para divulgar el siguiente mensaje: GOPdarse cuentaYa, te ha prometido un regalo de Navidad. Este es el comienzo del regalo. Por favor envíe un correo electrónico titulado "Feliz Navidad" a las direcciones que tengas, y dinos qué quieres en nuestro regalo de Navidad.

Cargos penales:

1. 18 USC § 371- Conspiración para cometer un delito o defraudar a Estados Unidos
2. 18 U.S.C. § 1030 - Código de los Estados Unidos - 18. Delitos y procedimientos penales § 1030. Fraude y actividades relacionadas en conexión con computadoras
3. 18 U.S.C. § 1349 - Código de los EE. UU. - 18. Delitos y procedimiento penal § 1349. Intento y conspiración

Definiciones de términos

1. Code: Según la acusación del Departamento de Justicia (2018), es un conjunto de instrucciones especialmente formateadas que dirigen al procesador de una computadora a manipular y almacenar datos. Un "programa", "software" o "archivo ejecutable" de la computadora son varias formas de referirse a un cuerpo completo de código binario que tiene un conjunto definido de funcionalidades.
2. Lista de Contactos: Según la acusación del Departamento de Justicia (2018), Los "contactos almacenados" o una "lista de contactos" son esencialmente la "libreta de direcciones" o Rolodex digital para una cuenta en línea. Estas listas a veces se completan automáticamente o pueden ser rellenadas manualmente por el usuario, dependiendo del correo electrónico particular, las redes sociales u otra comunicación proporcionar
3. DNS: Según la acusación del Departamento de Justicia (2018), El Servicio de nombres de dominio, o "DNS", es un sistema de nombres para computadoras, servicios o cualquier otro dispositivo.
4. DDNS: Según la acusación del Departamento de Justicia (2018), es un servicio ofrecido en el que el proveedor permitirá a los usuarios controlar la asignación de la dirección IP de un dominio, o más típicamente, un subdominio como <http://subdomain.domain.com>. El usuario puede acceder a esta asignación de dirección IP a través del proveedor y realizar cambios según sea necesario.
5. IP address: Según la acusación del Departamento de Justicia (2018), Una dirección de Protocolo de Internet versión 4, también conocida como "dirección IPv4", o más comúnmente una "dirección IP", es un conjunto de cuatro números u "octetos", cada uno

de los cuales va de 0 a 255 y separados por un punto (". ") Que se utiliza para enrutar el tráfico en Internet.

6. Malware: Según la acusación del Departamento de Justicia (2018), es un programa informático malicioso destinado a hacer que la computadora de la víctima se comporte de manera inconsistente con la intención del propietario o usuario de la computadora de la víctima, generalmente sin que la persona lo sepa.
7. North Korean IP Addresses: Según la acusación del Departamento de Justicia (2018), ciertas direcciones IP se denominan "norcoreanas". Esas referencias son a direcciones IP de dos bloques. El primero es un bloque de direcciones IP, 175.45.176.0–175.45.179.255, que están registradas en una empresa en Pyongyang, Corea del Norte. El segundo conjunto es un bloque de direcciones IP, 210.52.109.0–210.52.109.255, que, según múltiples fuentes disponibles públicamente, están registradas en una empresa en China, pero que Corea del Norte ha alquilado o utilizado desde antes de que Corea del Norte fuera asignó el primer bloque de direcciones IP a fines de 2009.
8. Phishing: Según la acusación del Departamento de Justicia (2018), un correo electrónico de "suplantación de identidad" suele ser uno que se envía a uno o más destinatarios y está diseñado para parecer legítimo con el fin de lograr que los destinatarios realicen una determinada acción, como hacer clic en un enlace o abrir un archivo que podría causar la computadora de una víctima debe ser comprometida por un hacker.
9. Proxy Service: Según la acusación del Departamento de Justicia (2018), un "servicio proxy" ofrece el uso de "servidores proxy", que son computadoras conectadas a Internet que sirven como retransmisores, a veces entre una persona que usa una computadora personal y el sitio web al que estaba accediendo. Cuando se utiliza un servicio proxy, los

sitios web a los que accede una persona generalmente no "ven" la ubicación de la dirección IP o país de origen "verdadero" o "local" donde se originó el tráfico de Internet, lo que revelaría la ubicación de la computadora de la persona.

10. Ransomware: Según la acusación del Departamento de Justicia (2018), El ransomware es un tipo de malware que infecta una computadora y encripta algunos o todos los datos o archivos en la computadora, y luego exige que el usuario de la computadora pague un rescate para descifrar y recuperar los archivos, o para evitar los actores maliciosos de distribuir los datos.
11. Recovery Emails: Según la declaración del Departamento de Justicia (2018), Los proveedores de correo electrónico y redes sociales con frecuencia requieren que los suscriptores enumeren una cuenta de correo electrónico "secundaria", "de recuperación" o "alternativa" al registrarse para obtener una cuenta de correo electrónico o de redes sociales. Las cuentas de correo electrónico de recuperación pueden ser utilizadas por un proveedor para autenticar que la persona que intenta acceder a la cuenta es, de hecho, el usuario autorizado para hacerlo.
12. URL: Según la declaración del Departamento de Justicia (2018), es una dirección de sitio web que se utiliza para dirigir una computadora a un servidor web en particular o un sitio web alojado en ese servidor web. Las URL pueden ser largas cadenas de palabras y caracteres, y algunas compañías, como Google, ofrecen "URL acortadas" que comprimen una URL completa en una cadena más pequeña de caracteres que es más fácil de encajar en mensajes de redes sociales como Twitter que limitan la cantidad de personajes que se pueden usar. Si se ingresa una URL acortada en un navegador web, el navegador web será redirigido a la URL completa.

13. Gusano: Según la declaración del Departamento de Justicia (2018), es un tipo de *malware* que intenta infectar progresivamente las computadoras, generalmente explotando una vulnerabilidad en las computadoras de las víctimas o mediante ataques de "fuerza bruta" en las computadoras de las víctimas. Un ataque de "fuerza bruta" en una computadora o red ocurre cuando un pirata informático o el *malware* del pirata informático intenta iniciar sesión en una computadora víctima potencial usando una lista predeterminada de posibles combinaciones de nombre de usuario y contraseña, que a menudo contienen miles de combinaciones comunes de nombres de usuario y contraseñas que incluyen configuraciones predeterminadas específicas utilizadas en ciertas aplicaciones y dispositivos.

SECCIÓN II: REVISIÓN DE LITERATURA

Introducción

La tecnología y los avances informáticos sin duda alguna no son el problema. Realmente, el problema está en el ser humano que con mente maliciosa la utiliza y la controla. La malicia y la conducta delictiva que se manifiesta en estas personas, son mediante la formulación de peticiones exclusivamente destinadas a obstruir y destruir.

Sin duda, podemos analizar que un hacker es una persona con un gran conocimiento de los sistemas y programas informáticos que conoce a detalle cada avance tecnológico y que busca siempre por supuesto, manipularlo de forma total.

Para Corey Nachreiner, director de Estrategia de Seguridad en WatchGuard, “hay tres tipos de hackers: los hacktivistas, que se organizan para los ataques, buscan mostrar la corrupción y el mal social y no tienen jefe; los ciberdelincuentes, pagados por el mejor postor, roban identidades y datos financieros, y son altamente peligrosos por sus métodos de extorsión; y finalmente los que trabajan para los gobiernos, que se dedican al *ciber* espionaje. Se trata de dañar enemigos y robar secretos industriales y federales,” según citado por Rojas (2014).

A continuación, se explica más a fondo los fraudes cometidos por Jin Hyok, un joven coreano que manejo a su antojo los sistemas de información logrando tener acceso a la base de datos de Sony Pictures, robando de ella películas que aún no tenían fecha de estreno y sientos de miles de información privilegia y comprometedora.

Fraudes Involucrados

Park creó un tipo de *ransomware* conocido como *WannaCry 2.0*, que afecto a toda Europa y a cientos de miles de computadoras. Según AVAST Software s.r.o (2015), el ransomware

(también conocido como rogueware o scareware) restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción. Los ataques más peligrosos los han causado ransomware WannaCry.

Según Jaimovich (2018), WannaCry comenzó un 12 de mayo de 2017 y fue descrito como un "ataque sin precedentes" por la magnitud que tuvo de atacar a más de 230 mil computadoras en 150 países. Los países más perjudicados fueron Rusia; Ucrania; India, Gran Bretaña, donde se vio comprometido el servicio nacional de salud de España y Alemania, donde la empresa ferroviaria alemana Deutsche Bahn AG fue el principal blanco de ataque.

Según Jaimovich (2018), WannaCry se propagó agresivamente usando la vulnerabilidad de Windows EternalBlue, o MS17-010. EternalBlue es un error crítico en el código de Windows de Microsoft que es al menos tan viejo como Windows XP. La vulnerabilidad permite a los atacantes ejecutar código de forma remota, creando una solicitud para el servicio de compartir archivos e impresoras de Windows.

Dirigiéndonos a los ataques a Sony Pictures, se sabe que se produjeron como resultado del enfado en Pyongyang por el estreno de la película "*The Interview*", una comedia sobre un intento de asesinato al dictador norcoreano Kim Jong-un. Los ataques fueron producidos a través de ataques informáticos (*Phishing*).

No solo Sony Pictures ha sido víctima de ataques informáticos. También la empresa Marvel Studios. Según AO Kaspersky Lab (2019), los estafadores hacen un seguimiento constante de los eventos mundiales y adaptan sus esquemas a ellos. Marvel fue víctima de

phishing cinematográfico en vísperas del lanzamiento de la última serie de Los Vengadores. Lo que ocasiono pérdidas millonarias para la compañía.

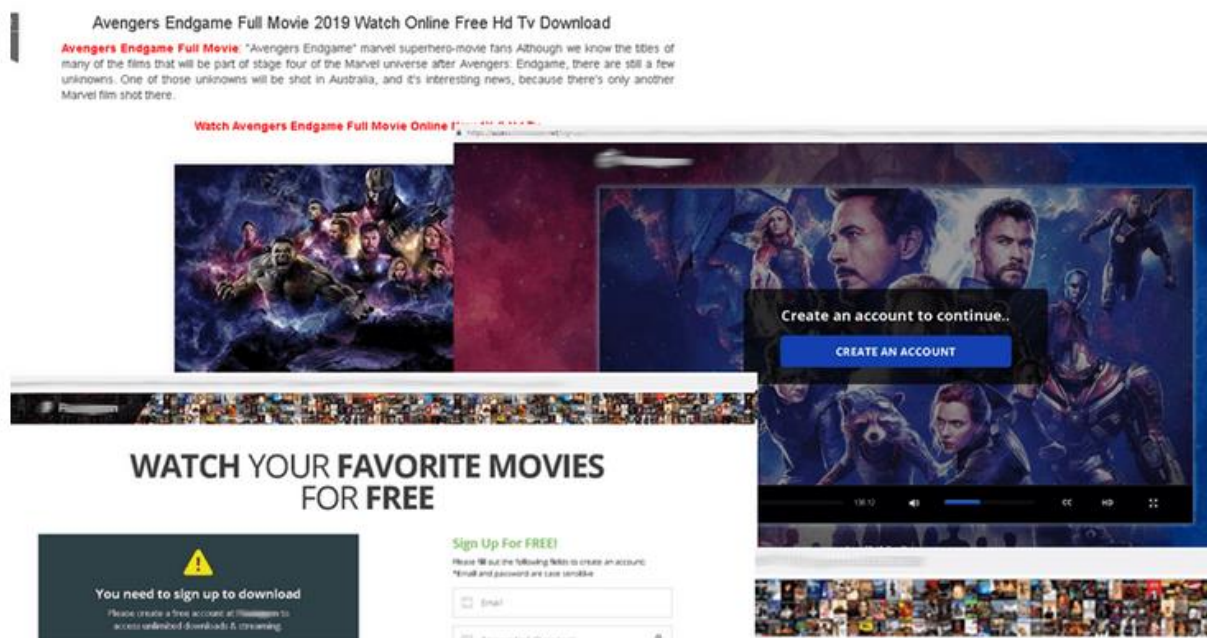


Figura 2: Presenta una página web que aparenta ser legítima, donde se pueden descargar películas gratuitas, que aún están en el cine o no han sido estrenadas por las casas productoras.

Estadísticas

AO Kaspersky Lab (2019) señala que los primeros puestos en la lista de países fuente de spam no han cambiado: en primer lugar, China (23,72%), el segundo lugar lo ocupó EE. UU. (13,89%), el tercer lugar le correspondió a Rusia (4,83%), Brasil ocupó el cuarto lugar (4,62%), y solo la quinta posición Francia (3,11%) que desplazó a Alemania.

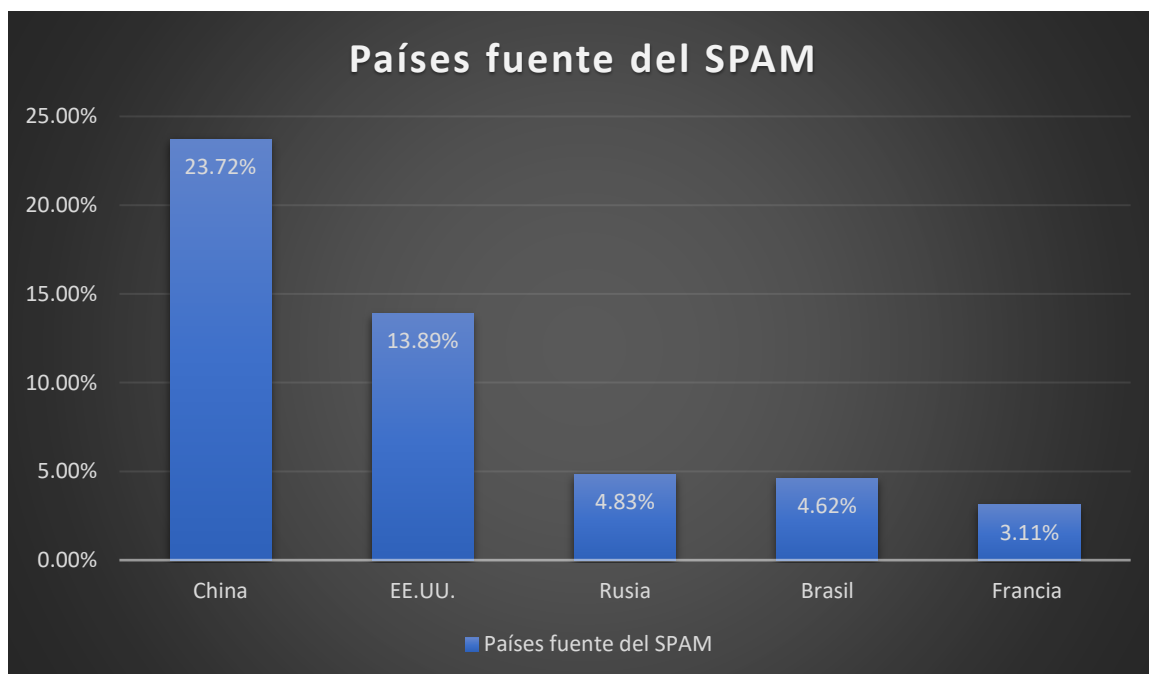


Figura 3: Grafica sobre los países que han sido fuentes de SPAM en el pasado 2019.

Según la Dirección de Protección de Datos (2012), a pesar de que la gran mayoría de los usuarios indican poder reconocer un correo de *phishing*, los datos demuestran que los ataques de esta índole aún tienen alta efectividad. Un claro ejemplo de esto es un *phishing* bancario que capturo 35 tarjetas de crédito en 5 horas. Es por esto que remarcamos la importancia de contar con una buena educación por parte de los usuarios y el uso de una solución de antivirus con capacidad de detección proactiva, que pueda identificar estos sitios maliciosos.

Según la Dirección de Protección de Datos (2012), los usuarios podrían reconocer si un correo es falso o no. Que un usuario pueda reconocer un correo de *phishing* es solo un 36,8% y de igual forma lo reporte a las entidades pertinentes ya que la gran mayoría simplemente borra el correo.

A continuación, una gráfica que nos muestra las principales vías del *phishing*.

¿De qué tipo de entidades suele recibir los correos que reconoce como falsos?

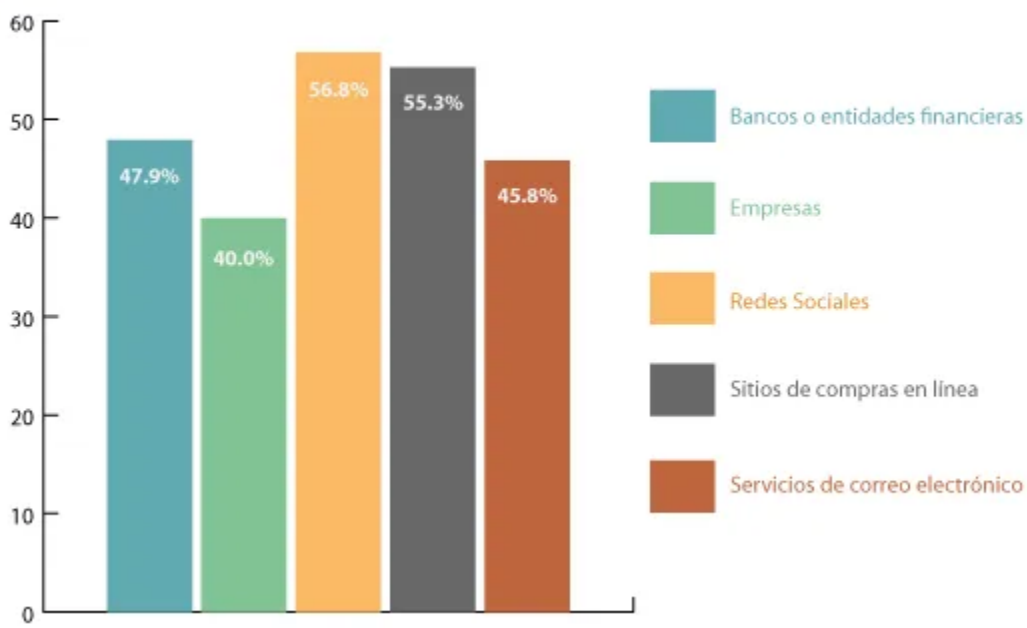


Figura 4: Estadística en porcentaje de cómo son presentados los correos electrónicos falsos.

Leyes aplicables

18 USC § 371- Conspiración para cometer un delito o defraudar a Estados Unidos

Según el Departamento de Justicia (2020), la sección 371 establece que si dos o más personas conspiran para cometer un delito contra los Estados Unidos , o para defraudar a los Estados Unidos , o cualquier agencia de 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.

18 U.S.C. § 1030 - Código de los Estados Unidos - 18. Delitos y procedimientos penales § 1030. Fraude y actividades relacionadas en conexión con computadoras

Según el Departamento de Justicia (2020), establece como delito el haber accedido a una computadora a sabiendas sin autorización o exceder el acceso autorizado, y por medio de dicha conducta haber obtenido información que ha sido determinada por el Gobierno de los Estados Unidos de conformidad con una orden ejecutiva o un estatuto para exigir protección contra la divulgación no autorizada por razones de defensa nacional o extranjera relaciones, o cualquier información restringida, como se define en el párrafo y. de la sección 11 de la Ley de Energía Atómica de 1954 , con razones para creer que dicha información así obtenida podría usarse para perjudicar a los Estados Unidos, o en beneficio de cualquier nación extranjera que comunique, entregue, transmita o haga que comunicado, entregado o transmitido, o intenta comunicarse, entregar, transmitir o hacer que se comunique, entregue o transmita lo mismo a cualquier persona que no tenga derecho a recibirlo, o retenga intencionalmente lo mismo y no lo entregue al oficial o empleado de los Estados Unidos con derecho a recibirlo.

18 U.S.C. § 1349 - Código de los EE. UU. - 18. Delitos y procedimiento penal § 1349. Intento y conspiración

Según Justicia US Law (2012), establece que cualquier persona que intente o conspire para cometer un delito en virtud de este capítulo estará sujeta a las mismas sanciones que las prescritas para el delito, cuya comisión fue o haya sido el objeto del intento o la conspiración.

Casos relacionados

1. Departamento de Justicia de los Estados Unidos Vs. Ardit Ferizi, aka Th3Dir3ctorY

Según la declaración del Departamento de Justicia (2016), las autoridades de Malasia han arrestado a un joven llamado Ardit Ferizi, de 20 años de nacionalidad kosovar, se le acusa de ser

autor del robo de datos de los ordenadores de las fuerzas de Seguridad Nacional de Estados Unidos y, enviarlos al estado Islámico. El Departamento de Seguridad Nacional de los Estados Unidos, es un ministerio del Gobierno de los Estados Unidos, con la responsabilidad de proteger el territorio estadounidense de ataques terroristas y responder a desastres naturales. Se afirma que Ferizi, proporcionó apoyo material a ISIS y cometió ataques informáticos y robo de identidad.

Ardit Ferizi, detenido durante una redada de la policía antiterrorista, había entrado en el país asiático en agosto para estudiar informática en una universidad privada de Kuala Lumpur, el acusado, que usaba el nombre en clave de “Th3Dir3ctorY” dirigía una red de piratas informáticos kosovares llamada 'Kosova Hacker's Security' (KHS), y se calcula que había conseguido robar las direcciones de correo electrónico, las contraseñas, sus direcciones postales y números de teléfono de más de 1,300 miembros de las fuerzas armadas estadounidenses. Más tarde, el 13 de agosto, un empleado de una de las empresas pirateadas por Ferizi, denunció un acceso ilegal a sus servidores. Seis días después, el FBI fue contactado por un mensaje amenazante enviado por Ferizi, a una de sus víctimas. Esto ocasiono que los Estados Unidos solicitara inmediatamente la extradición de Ferizi, para poder procesarlo en territorio americano.

2. Tribunal de los Estados Unidos para el Distrito Sur de Indiana Vs. Fujie Wang

Según Cyber Security (2019), el 7 de mayo de 2019, un gran jurado en el Tribunal de los Estados Unidos para el Distrito Sur de Indiana, División de Indianápolis, acusó a dos personas de conspiración para cometer fraude y actividades relacionadas en conexión con ordenadores, conspiración para cometer fraude electrónico y causar intencionalmente daño a un dispositivo protegido. Los sujetos, incluido Fujie Wang, eran presuntos miembros de un grupo de cibercriminales que operaba en China y realizaba campañas de intrusión dirigidas a los sistemas informáticos de grandes empresas en los Estados Unidos, incluida una gran empresa del sector

salud en Indiana. Se alega que, entre febrero de 2014 y enero de 2015, los sujetos conspiraron para acceder intencionalmente a redes informáticas para identificar y robar datos sobre aproximadamente 78.8 millones de personas de redes informáticas, incluidos nombres, números de identificación de salud, fechas de nacimiento, números de la Seguridad Social, direcciones, números de teléfono, direcciones de correo electrónico, información de empleo y datos de ingresos. Una vez que se recopiló la información, se colocó en un archivo cifrado y se envió a destinos en China.

3. Departamento de Justicia de los Estados Unidos Vs. Andrei Tyurin

Según Digital Security (2019), Andrei Tyurin es el hombre de nacionalidad rusa que se ha declarado culpable de una de las brechas de seguridad más importantes de una institución financiera estadounidense, el ciberataque contra JPMorgan Chase en 2014 que generó el robo de cientos de millones de dólares en ingresos ilícitos y de datos personales de más de 80 millones de clientes de la entidad financiera.

El ciberdelincuente, de 36 años y extraditado hace un año desde Rusia, ha sido acusado de robar información de clientes de doce compañías de información financieras, bancos y otras firmas, incluidas Fidelity Investments, E-Trade Financial y Dow Jones & Co. Sus socios usaron la información para atraer clientes con correos electrónicos no deseados. Tyurin se ha declarado culpable de intrusión informática, fraude electrónico, fraude bancario y juego online ilegal como según publica el Departamento de Defensa de Estados Unidos.

Según Digital Security (2019), el fiscal federal de Manhattan, Geoffrey S. Berman, ha mencionado la brecha de JP Morgan, como “uno de los mayores robos de datos de clientes de Estados Unidos de una sola institución financiera en la historia” y asegura que “el reinado de

intrusiones informáticas de Tyurin ha terminado y se enfrenta a un tiempo significativo en una prisión de Estados Unidos por sus crímenes”. Tyurin ha confesado que llevó a cabo los ciberataques siguiendo las instrucciones de Gery Shalon, quien utilizó los datos robados para realizar una serie de acciones, como fraude de valores, que implica inflar artificialmente el precio de ciertas acciones que cotizan en bolsa comercializándolas de manera engañosa a los clientes de las empresas que Tyurin había pirateado previamente.

Herramientas de investigación

Para el estudio y análisis de un caso debemos tener en cuenta las herramientas que utilizáramos y si serán efectivas para el tipo de investigación que deseamos realizar. Se pretende utilizar:

1. **OSForensic** – según Proteger mi PC (2018), OSForensic es una pieza clave en investigaciones forenses digitales permite localizar pistas, mirar en el interior de archivos y sus cabeceras y, finalmente, organizar e indexar todos los datos hallados para un tratamiento posterior y su presentación.
2. **FTK** - según Technology INT, FTK es una plataforma de investigaciones digitales aprobada por tribunales. Recopila datos de cualquier dispositivo o sistema digital que produzca, transmita o almacene datos; y realiza el análisis forense de los mismos. FTK es conocido por su interfaz intuitiva, su análisis de correo electrónico, las vistas de datos personalizables, su velocidad de procesamiento y su estabilidad.

SECCIÓN III: SIMULACIÓN DEL CASO

La conspiración y los ataques a Sony Pictures, fue uno sin precedentes y de gran impacto para la casa productora. Un pirata informático Park Jin, obtuvo acceso a la red privada de SPE, enviando *malware* a los empleados para luego robar datos confidenciales como: credenciales, correos electrónicos, contraseñas, películas sin estreno y un sin número de información personal de los empleados. Los programas malignos enviados por Park, a SPE contenían *scripts* diseñados para atacar los sistemas operativos de las computadoras deseadas.

El ataque a Sony Pictures se produjo por la publicación de un nuevo filme de película, titulada “The Interview”. Esta película desato la ira del gobierno coreano y causó un gran malestar en el país asiático, porque fue considerada como una burla al líder del país, Kim Jong-Un. El ataque comenzó en noviembre de 2015, cuando Park utilizó cuentas falsas de correo electrónico enviando mensajes de phishing con *software* malicioso a los empleados de Sony, para debilitar el sistema operativo dejándolo vulnerables y hacer completamente inoperantes la mayoría de sus computadoras.

El motivo principal, además de demostrar fuerza, soberanía y control por parte del país asiático; era evitar que SPE llevara a cabo el lanzamiento de la película “The Interview”., intentando realizar un sabotaje. Park, envió un mensaje amenazante a empleados de Sony, indicándole que tenían *email* que comprometían a SPE y haría público un paquete de información robada que contiene más de 12.000 *emails* de la cuenta de correo electrónico de Michael Lynton, presidente de SPE. Logró que algunas de las principales cadenas de cines de los Estados Unidos informaran que renunciaban a la exhibición de filme ya que, si no, harían

público un paquete de información robada de la cuenta de correo electrónico de Michael Lynton, presidente de SPE.

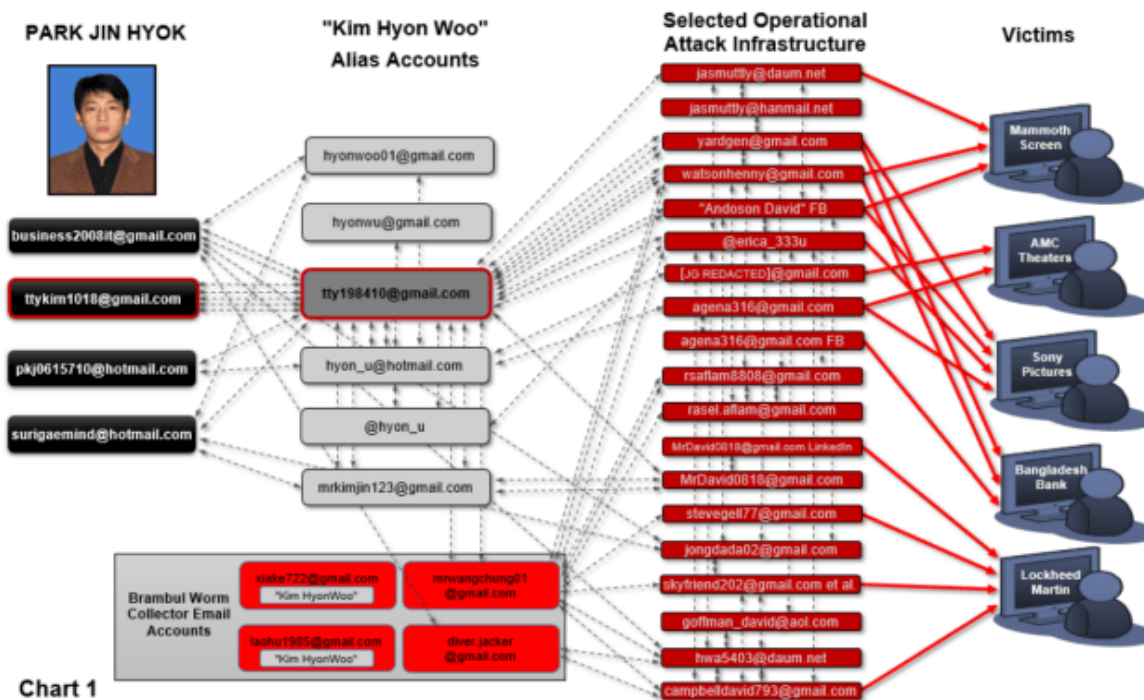


Figura 5: Diagrama que relaciona a Park Jin Hyok con sus víctimas.

En el diagrama de la *figura 6*, podemos ver el proceso de cómo se llevó a cabo el delito. Comencemos por el acusado Park Jin, quien fue la mente maestra para el ataque, aun sin número de entidades incluyendo la de Sony Pictures. Park, creaba email con cuentas falsas que parecieran confiables para enviar correos electrónicos con programas malignos o virus (gusanos), para poder tener acceso a las máquinas deseadas colocando en esos correos *links*, páginas de interés o simplemente enviando *script* que contenían códigos de programación, con el motivo de que fueren abiertos y poder lograr acceso a toda información. Por consiguiente, estos *emails* eran enviados a personas específicas de interés para Park. Para lograr esto, también utilizó el programa Proxy el cual le permitía lograr entrar a los ordenadores de forma remota. Esto provocaba copias de

seguridad en las páginas que accedían los empleados de Sony, para luego Park visitarlas y obtener la información deseada.

Simulación de Fraude

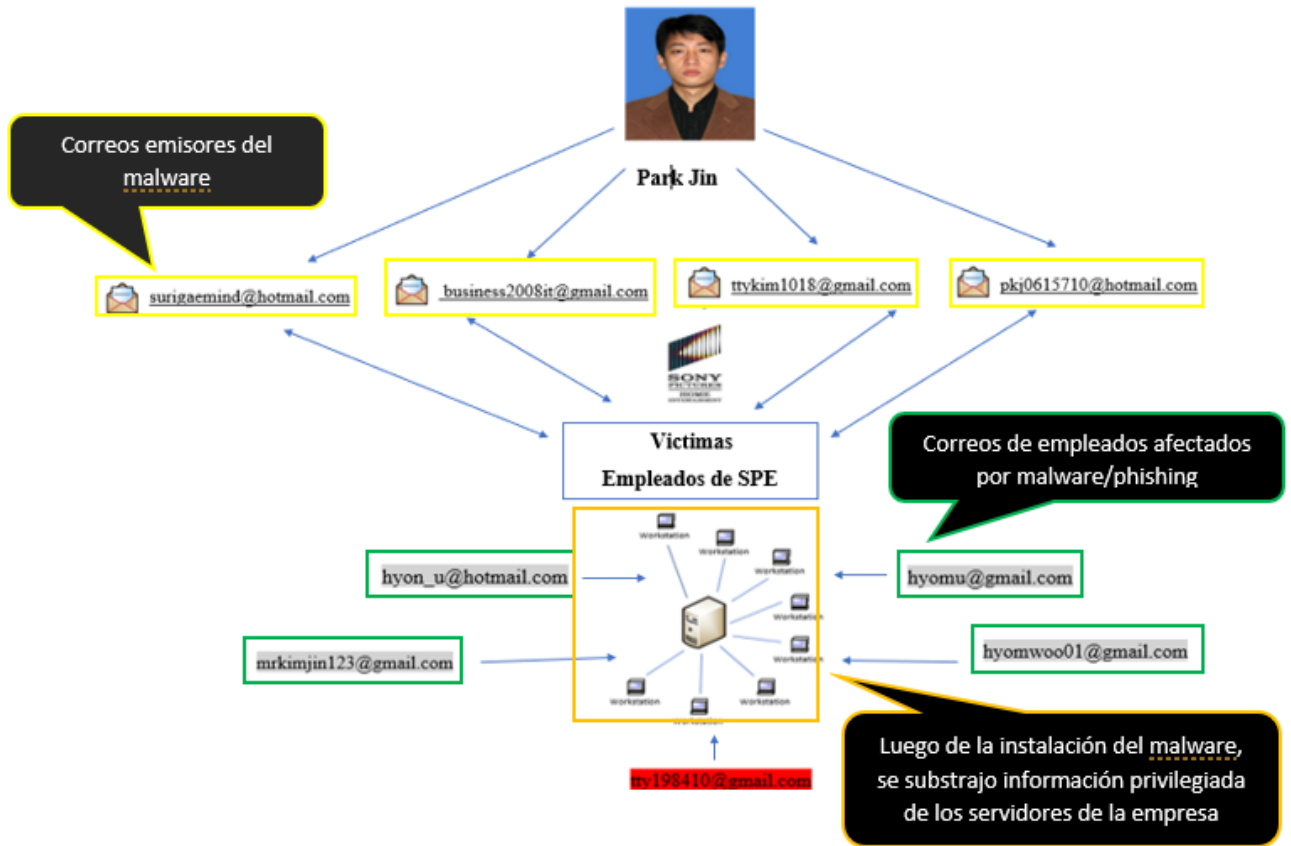


Figura 6: Diagrama que simula el proceso del delito.

SECCIÓN IV: INFORME FORENSE DEL CASO

Resumen Ejecutivo

Tracy Wilkison, primer fiscal general adjunto de los Estados Unidos para el distrito de California, contrató los servicios de Law Forensic System para el análisis del disco duro de una computadora que fue incautada como evidencia en el allanamiento realizado por parte del FBI en la casa productora Sony Pictures Entertainment Inc en busca de evidencias. Esa pieza de evidencia es clave para el análisis de obtención de prueba ya que la mayoría de las computadoras quedaron inoperantes ante el alegado ataque por parte de Park Jin que causo el colapso del sistema operativo de la gran mayoría de las computadoras.

Como parte de la examinación del disco duro, se identificaron archivos que fueron borrados, acceso a páginas de internet, direcciones de IP y correos electrónicos. Las pruebas obtenidas pretenden relacional al acusado con el atentado a Sony Pictures.

Al finalizar el análisis del disco duro, se entregó al fiscal a cargo John C. Demers, fiscal general adjunto de Seguridad Nacional de la corte de California. Junto a la evidencia se entregaron los hallazgos y el informe sobre el análisis.

Objetivo

Se contratan los servicios de Law Forensic System, por parte de la corte de California para la examinación y análisis del disco duro incautado en Sony Pictures, para el hallazgo de evidencias. El objetivo principal es encontrar toda evidencia inculpatoria que muestre la participación de Park Jin, con los hechos relacionados al ataque de Sony Pictures.

Alcance del trabajo

El 21 de febrero de 2020, el Fiscal Tracy Wilkison, primer fiscal general adjunto de los Estados Unidos para el distrito de California, hizo entrega a la examinadora experta Noemí Caba Calderón, un disco duro marca GLYPH Blackbox Pro. Dispositivo fue removido de una computadora confiscada por parte del Agente Tracy Wilkison, en la empresa de Sony Pictures, en California.

Se espera un análisis completo del disco duro donde se obtenga todos los datos existentes o borrados que hagan alguna conexión con el acusado. Como parte de la investigación y análisis se requiere utilizar herramientas de examinación aprobadas por el tribunal. Se utilizó OSForensics, una herramienta de Software que permite investigar cualquier clase de información contenida en un soporte informático, tanto visible como oculta adquiriendo la evidencia necesaria para análisis.

Datos del caso

- **Número de caso:** MJ 18-1479
- **Investigador:** Nathan P. Shields, agente especial de la Oficina Federal de Investigación
- **Cliente solicitante de la investigación:** Noemí Caba Calderón
- **Representante del cliente:** Christopher A. Wray, abogado y director del FBI.

Descripción de los dispositivos utilizados

A continuación, se describen los dispositivos que fueron utilizados para la examinación forense:

1. Computadora Toshiba modelo Satellite C55 DT-B, con procesador AMD A8-6410 APU with ADM Radeon R5, número de producto 00326-10000-00000-AA679 y sistema de 64

bit. Esta computadora contiene el programa OSForensics, el cual se estará utilizando para la examinación del disco duro.

2. Disco duro modelo GLYPH Blackbox Pro, número de serie PRO1901022515 con 10 TB.

EVIDENCE	
Submitting Agency:	Corte de California
	Departamento de Justicia
Case No:	NJ 18-1479
Item No:	MJ 032903
Date:	02/21/2020
Time:	02/21/2020 - 7:30 AM
Collected By:	Tracy Wilison
Bag No:	03321
Evidence Description:	Disco duro modelo Glyph Blackbox Pro #serie PRO1901022515 con 10TB
Location:	California US.
Type of Offense:	Crimer Cibernetico
Victim's Full Name:	Sony Pictures
Suspects Full Name:	Park Jin
PAPER PRINTING INC. No. 03321	




Figura 7: Entrega de evidencia del Disco duro GLYPH Blackbox Pro.

Resumen de hallazgos

A continuación, se mostrarán los hallazgos durante el proceso de examinación del disco duro.

1. Se encuentra en el almacén de seguridad del disco duro, un intento fallido de autenticación (*Figura 8*). Se revela el número de dirección de IP del cual se intentó acceder de forma remota.

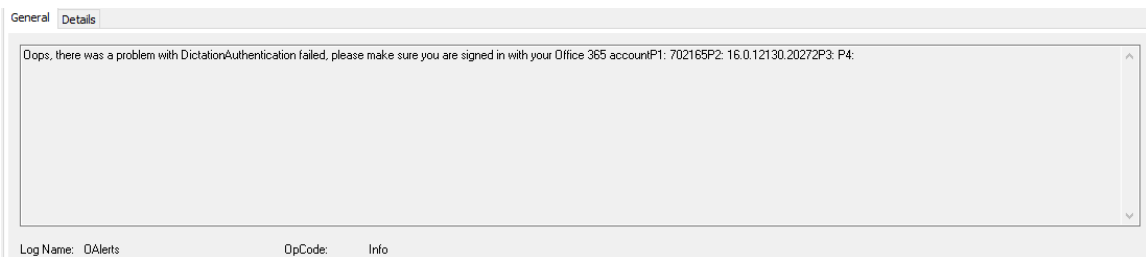


Figura 8: Intento de autenticación fallido.

2. Se encuentra seis eventos de error donde se demuestran intentos de acceso al DESKTOP-2QEUG3J (*figura 9*) los cuales fueron denegadas.

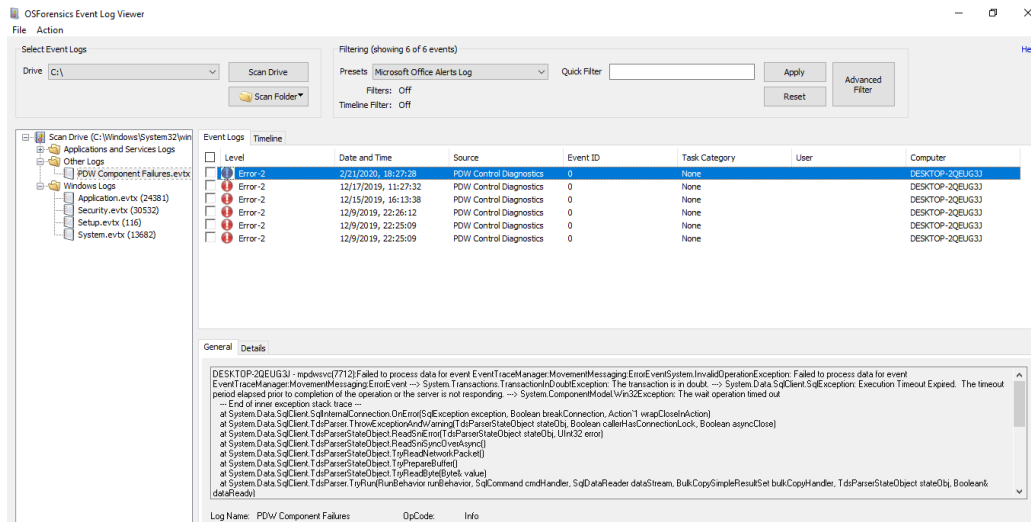


Figura 9: Intentos de acceso a DESKTOP-2QEUG3J perteneciente a empleado de SPE.

3. Se encuentra lista que detalla las entradas a correos electrónicos (*figura 10*). Se describen por fecha y hora de acceso.

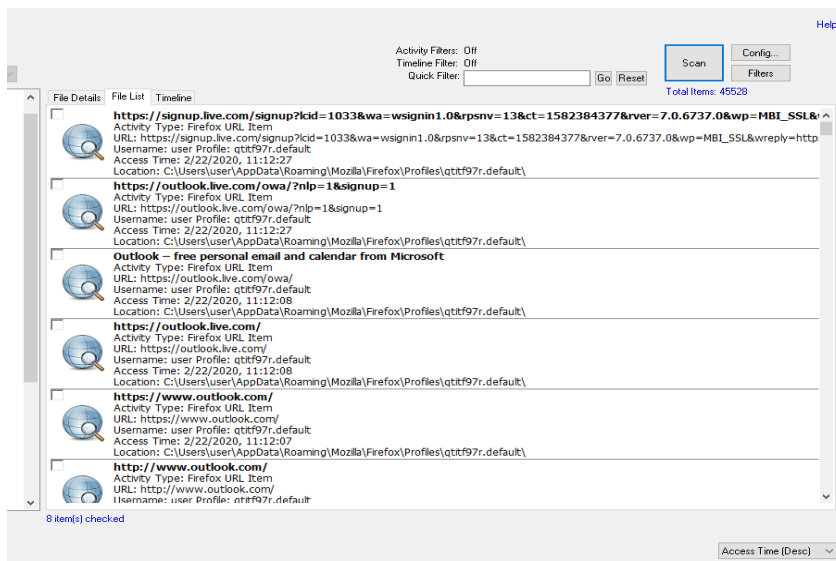


Figura 10: Actividad de acceso a correos electrónicos.

4. En el análisis de los correos electrónicos enviados por el acusado, se encontraron varios correos amenazantes, los cuales fueron borrado de forma remota. Algunos de ellos enviados a nombre de “Frank David” (*figura 11*) y otro a nombre de bussiness bussiness.



Figura 11: Correo electrónico amenazante por parte del acusado.

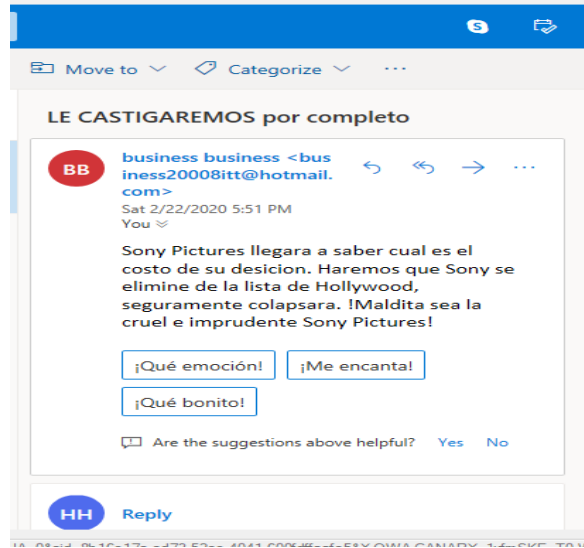


Figura 12: Correo electrónico amenazante enviado a empleado de Sony.

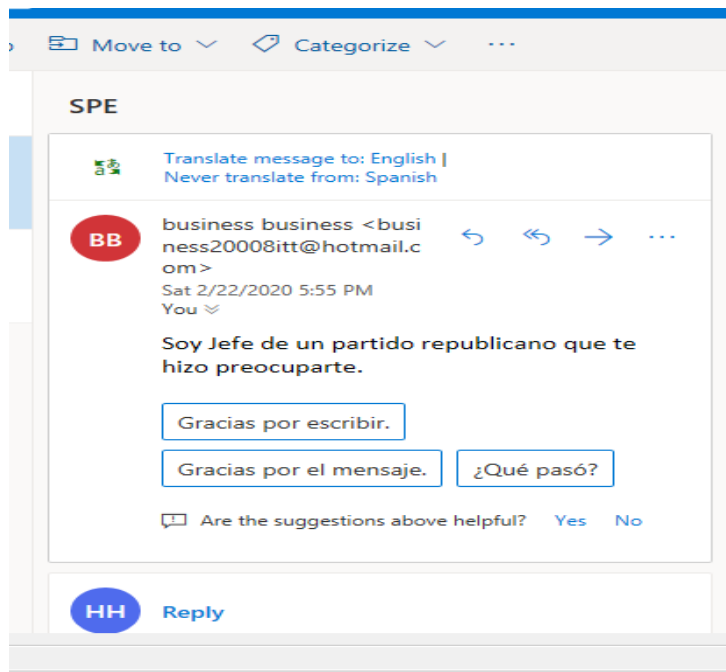


Figura 13: Correo electrónico amenazante.

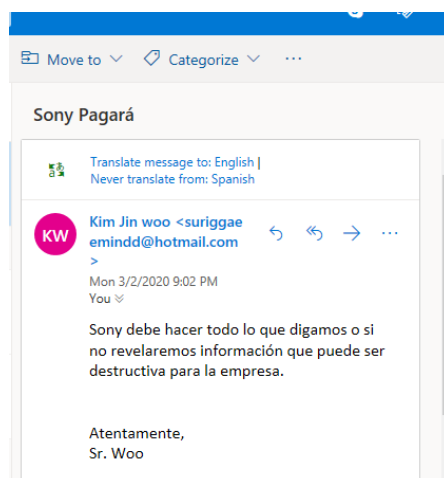


Figura 14: Se identifica correo enviado a empleado de Sony donde se presenta el mismo apellido del acusado.

5. En la búsqueda en la base de datos de SPE, se encontró un pareo positivo con un currículum entregado por un aspirante llamado Jin Hyok Park, el 17 de febrero del 2003, esto para una vacante en la empresa. En este currículum se encontraba datos exactos de información personal y de contacto del aspirante Jin Hyok Park, acompañado de una foto. La dirección de correo utilizada en el currículum forma parte de los correos utilizados en los ataques contra SPE (figura 15).



Jin Hyok Park
Sometown, MI 48901
453.856.2898

suriggaemindd@hotmail.com | LinkedIn URL | Twitter Handle

DATABASE DEVELOPER

Diligent and productive database developer with a high level of work integrity. Backed by solid credentials, technical acumen and an exemplary-rated work history in database development.

Experience developing server-side database management system (DBMS) applications on multiple platforms. Maintain security infrastructure and best practices.

Proven success designing high-integrity relational/dimensional databases and business intelligence solutions supporting critical business areas.

Skills

Visual Studio | .Net | C# | VBA for Access | ASP | ASP.NET | SQL Server | Transact-SQL Oracle | SSIS | SSAS | SSRS | SAP ASE | Ingres | MDX | C++ | C | Perl | MS Access

Database Development | BI Solutions | Data Warehousing & Integration | Object & Dimensional Modeling OLAP & OLTP Data Modeling | Scripting, Coding & Documentation

Professional Experience

ABC Company, Electronics reseller and distributor with a global clientele

Database Developer, 6/1997 to Present

Junior Database Developer, 9/1992 to 6/1997

Define system/user requirements to design, develop, document, test and implement data models, database architecture and DBMS/BI solutions supporting sales, marketing, ecommerce, finance, customer service, billing and other crucial business functions.

Key Accomplishments:

Developed new and customized existing databases using a variety of technologies, languages and programming tools.

Worked on team and individual development projects to deliver secure, robust and scalable DBMS/BI solutions that helped improve efficiency, information security, data integrity and customer satisfaction.

Partnered with Web developers to create database-backed Web site that accelerated customer order fulfillment sixfold and elevated ecommerce sales by \$850K in three months.

Identified and rectified a programming flaw in core CRM database. Prevented the irretrievable data loss of dozens of product orders totaling more than \$150K.

Education

XYZ University -- Sometown, MI

BS in Information Technology (Database Emphasis), Minor in Math



Figura 15: Currículo que involucra a Park con los hechos contra SPE.

6. Muestra reporte de actividad en correos electrónicos (*Figura 16*), y detalles en tiempo y hora.



Figura 16: Reporte sobre actividad en correos electrónicos.

7. Se confirma que desde la computadora de Sony Pictures un usuario no autorizado penetra de forma remota a la computadora y accedió a la página de internet “PASTEBIN” donde se descargó un *malware* que le permite extraer información de las computadoras (figura 17)

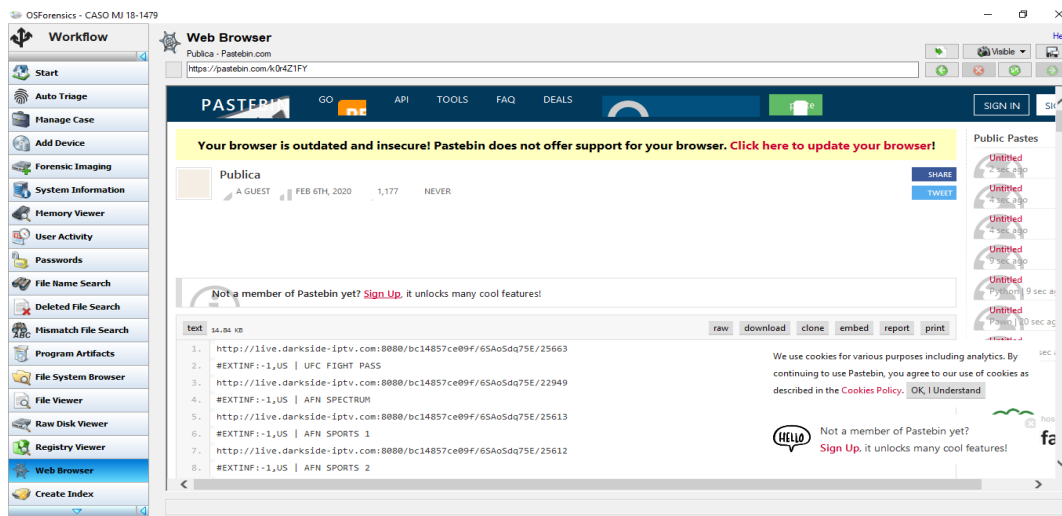


Figura 17: Acceso a página de internet “PASTEBIN”.

Cadena de custodia

Law Forensic System, garantiza la autenticidad, seguridad, preservación e integridad de la evidencia física hallada o colectada que ha sido examinada. Todas las pruebas se examinan de manera continua e interrumpida, hasta que esta sea entregada como elemento de prueba ante un tribunal.

Primer Evento

- Descripción: Evidencia recibida del fiscal Tracy Wilkison, primer fiscal general adjunto de los Estados Unidos para el distrito de California.
- Verificado por: Noemí Caba Calderón
- Fecha de comienzo: 20 de febrero de 2020
- Fecha de terminación: 20 de febrero de 2020
- Lugar de Origen: Corte del distrito de California
- Estado de la evidencia: Dentro de una bolsa transparente sellada con etiquetas de confidencialidad.
- Destino: Laboratorio forense - Law Forensic System

Segundo Evento

- Descripción: Se crea proyecto con el número de caso para análisis forense.
- Verificado por: Noemí Caba Calderón
- Número de caso judicial: MJ 18 1479
- Número de caso a trabajar para expediente: MJ181479-02212020
- Fecha de comienzo: 21 de febrero de 2020 – 10:12 AM.
- Fecha de terminación: 21 de febrero de 2020 – 10:25 AM.

- Lugar de Origen: Laboratorio forense - Law Forensic System
- Destino: Laboratorio forense - Law Forensic System

Tercer Evento

- Descripción: Búsqueda de evidencia y análisis forense.
- Verificado por: Noemí Caba Calderón
- Número de caso judicial: MJ 18 1479
- Número de caso a trabajar para expediente: MJ181479-02212020
- Fecha de comienzo: 21 de febrero de 2020 – 10:30 AM.
- Fecha de terminación: 27 de febrero de 2020 a las 1:20 PM.
- Lugar de origen: Laboratorio forense - Law Forensic System
- Destino: Laboratorio forense - Law Forensic System

Cuarto Evento

- Descripción: Se entrega la evidencia a Tracy Wilkison, primer fiscal general adjunto de los Estados Unidos para el distrito de California.
- Verificado por: Noemí Caba Calderón
- Número de caso judicial: MJ 18 1479
- Número de caso a trabajar: MJ181479-02212020
- Fecha de comienzo: 27 de febrero de 2020 – 3:00 PM.
- Fecha de terminación: 27 de febrero de 2020 – 4:05 PM.
- Estado de la evidencia: Dentro de una bolsa transparente sellada con etiquetas de confidencialidad.

- Destino: Tribunal del estado de California

Procedimiento

A continuación, se mostrará la herramienta y los pasos ejecutados que fue utilizado como parte del análisis para la obtención de evidencia física forense.

1. Procedimiento: Creación de caso

- Herramienta: OSForensics
- Fecha de comienzo: 21 de febrero de 2020
- Hora de comienzo: 10:12 AM.
- Fecha de Terminación: 21 de febrero de 2020
- Hora final: 10:25 AM.
- Descripción: Crear expediente de caso a examinar MJ 18 1479, donde se estará analizando disco duro confiscado de la empresa Sony Pictures, para evaluación forense y obtención de evidencia física.

2. Procedimiento: Análisis del caso

- Herramienta: OSForensics
- Fecha de comienzo: 21 de febrero de 2020
- Hora de comienzo: 10:30 AM.
- Fecha de terminación: 27 de febrero de 2020
- Hora final: 4:05 PM.
- Descripción: Se analiza toda información contenida en el disco duro. Incluyendo y no limitándose a información borrada, archivos que puedan estar encriptados y todo tipo de información útil para el proceso de examinación.

OSForensics es la herramienta utilizada para el análisis de evidencia que permite de una forma rápida, fácil y segura para la organización de datos creando informes que ayudaran a la presentación de evidencia ante el tribunal.

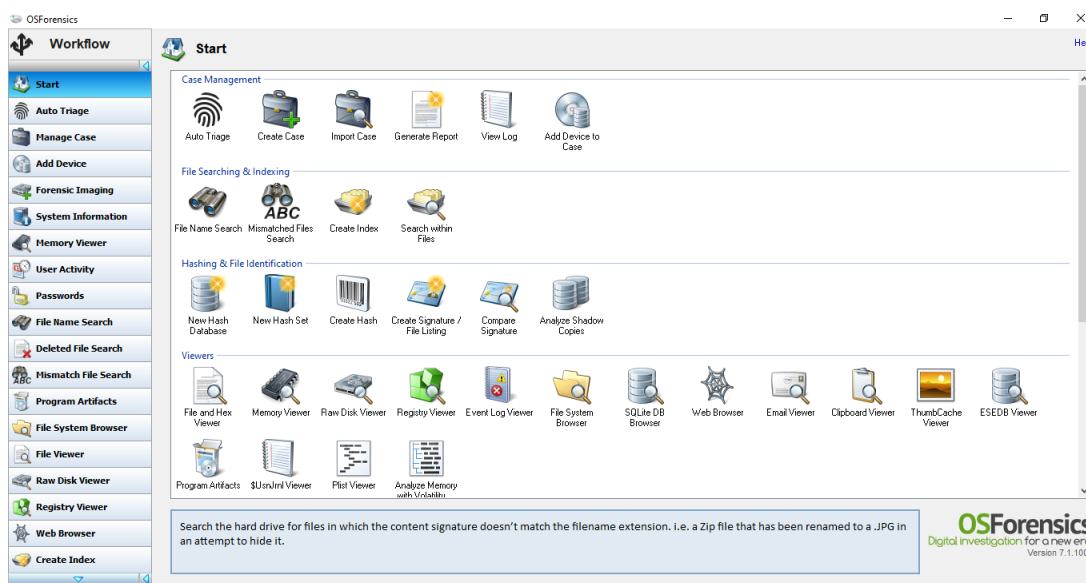


Figura 18: Plataforma de OSForensics.

1. Se muestra la extracción de la información del disco duro al programa OSForensics (Figura 19). La misma es presentada como un *summary* donde organiza por categoría toda la data que contiene el disco duro.

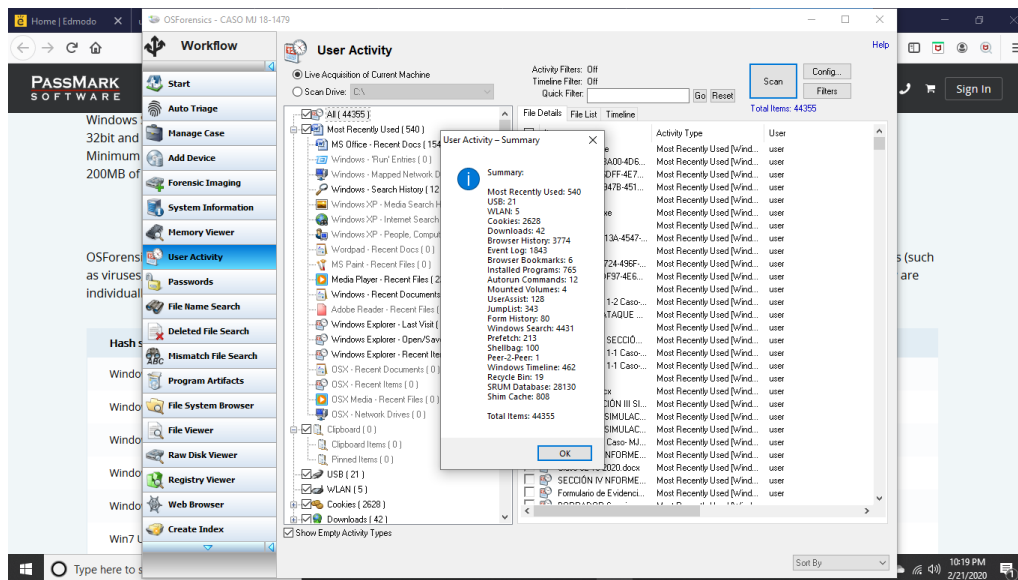


Figura 19: Extracción de información para análisis.

- Para poder tener el control de la evidencia encontrada se debe crear un expediente dentro de la plataforma donde se guarden todos los hallazgos del caso. Esto permitirá tener organizada la evidencia para tenerla accesible y clara para los informes finales (figura 20).

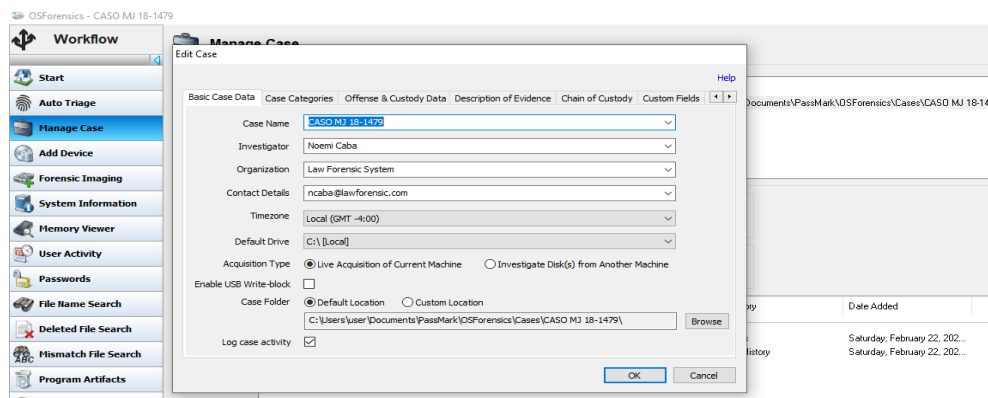


Figura 20: Iniciando análisis y creando expediente.

3. Luego de crear el caso nos permite organizar la evidencia entrada por categorías, esto nos ayuda a tener búsquedas más precisas para llevar una contabilidad de esa evidencia (figura 21).

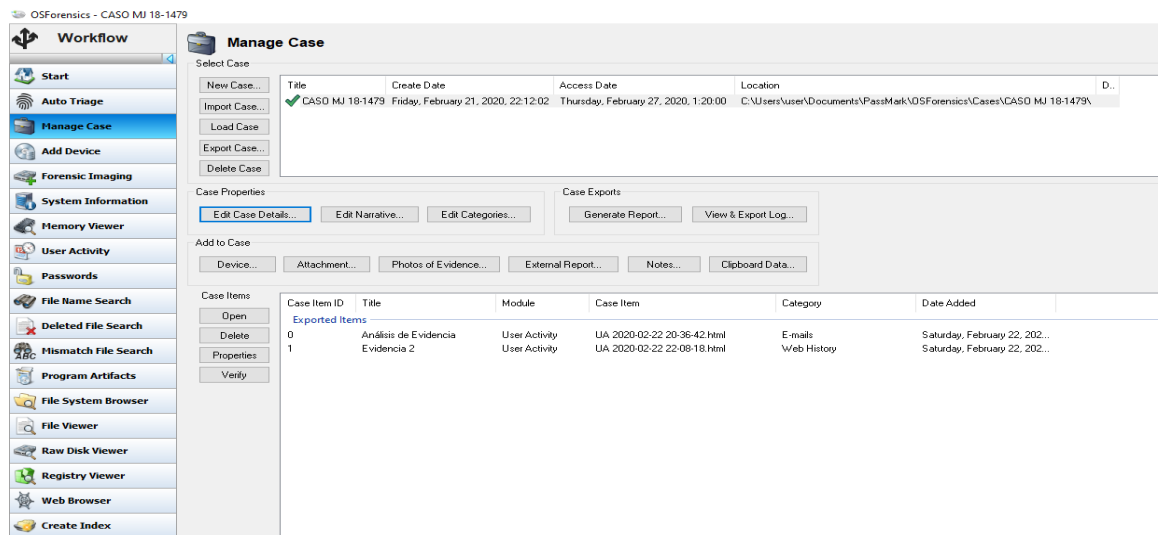


Figura 21: Organización de expediente por categorías.

4. En el análisis de los correos electrónicos recibidos, se encontraron varios correos amenazantes, los cuales fueron borrado de forma remota. Algunos de ellos enviados a nombre de “Frank David” (figura 22) y otro a nombre de bussiness bussiness (figura 23, 24 y 25).

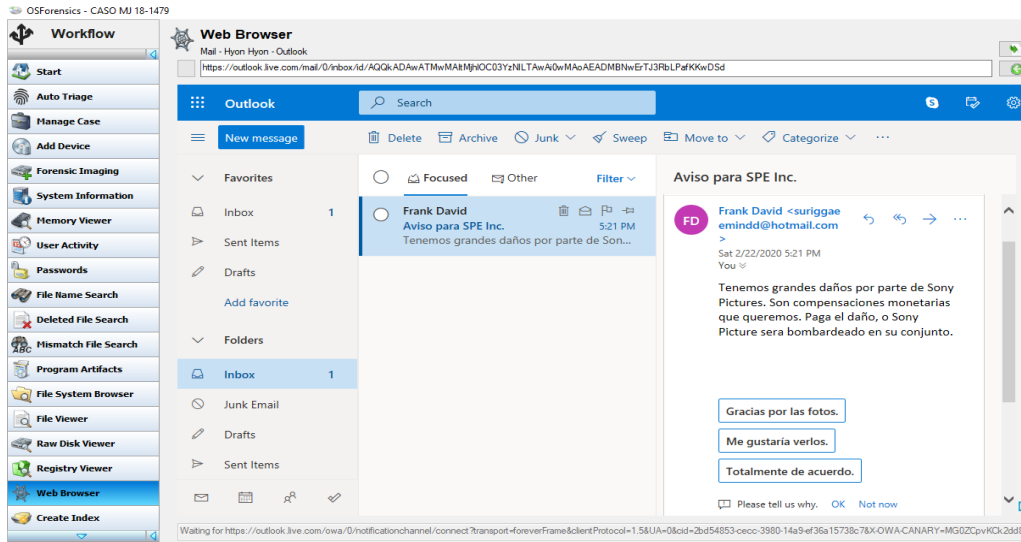


Figura 22: Correo electrónico amenazante por parte del acusado.

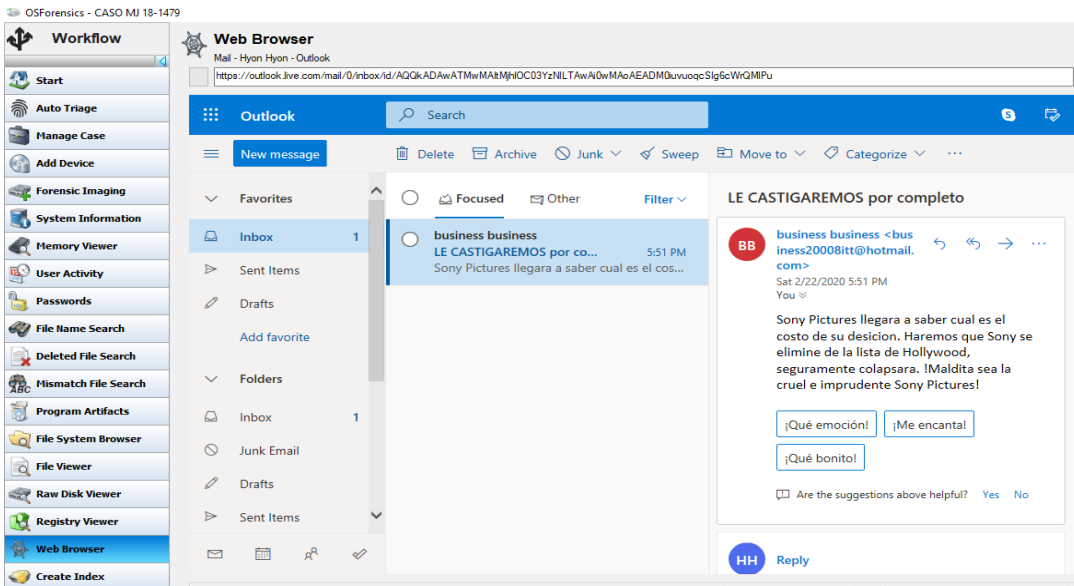


Figura 23: Correo electrónico amenazante por parte del acusado.

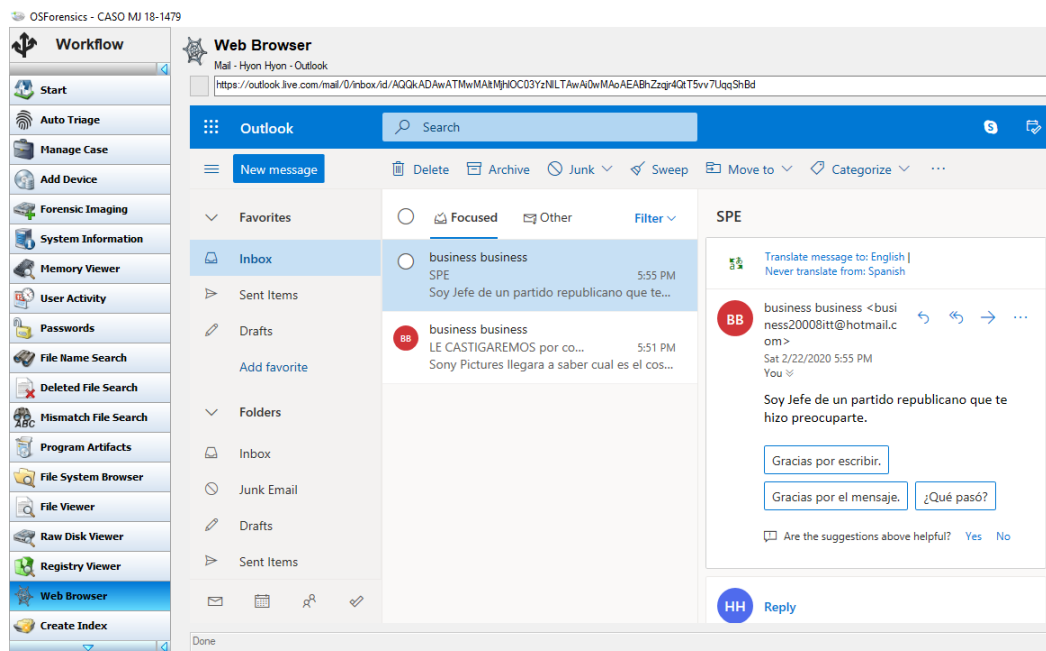


Figura 24: Correo electrónico amenazante a empleado de Sony.

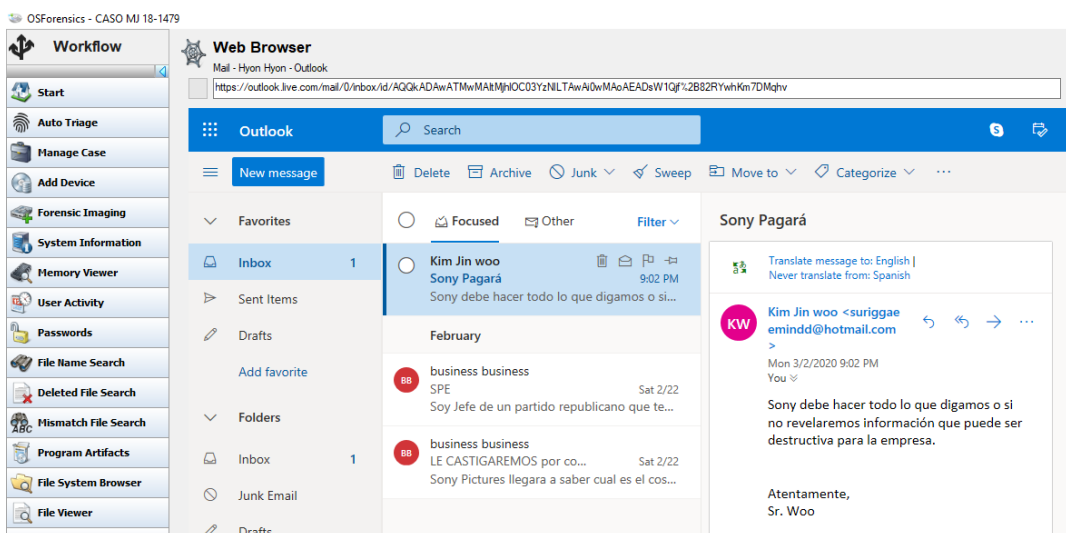


Figura 25: Correo electrónico enviado por “Kim Jin Woo”.

Conclusión

Luego de un extenso análisis del disco duro confiscado el cual contiene la base de datos de la empresa de Sony Picture. Se encuentra, evidencia explicita que señala directamente al Sr. Park como autor de los ataques sufridos a SPE del pasado noviembre de 2014. La evidencia demuestra que se utilizaron direcciones de IP para lograr acceso de forma remota a las computadoras, se demuestra que se logró acceso a través de correos electrónicos enviados a empleados con programas malignos tomando el control de sus terminales. También, que se logró acceso a los servidores logrando acceder desde la página internet llamada “PASTEBIN” donde se descargaban virus (gusanos) para dañar las computadoras volviéndolas vulnerables e inoperables luego del saqueo. Generando una gran cantidad de tráfico de información, a tal punto que hicieran explotar las vulnerabilidades existentes en aplicaciones de uso constante, permitiéndole acceder de una computadora a otra sin interrupciones.

El 17 febrero del 2003 SPE recibió un currículum de un aspirante llamado Park Jin, para una vacante en la empresa. La dirección de correo electrónico adjunta a este currículum, coincide con uno de los correos electrónicos involucrados en los ataques a Sony Pictures Entertainment Inc. El currículum contenía información exacta del Sr. Park que lo relaciona directamente con los ataques. Esto demuestra el manejo directo del *email* de Park.

SECCION V: DISCUSIÓN DEL CASO

La investigación surge por una acusación por parte de la casa productora de Sony Pictures, donde alega una intromisión en su sistema operativo y la pérdida de información. Se trata de un pirata informático, que logró acceso a la red de información de la casa productora de Sony Pictures. Esta investigación implicó la verificación y análisis del sistema operativo completo incluyendo y no limitándose a toda computadora utilizada por los empleados que pudieron haber sido fuentes de información.

Se analizaron correos electrónicos, páginas web y análisis de direcciones de IP. En los hallazgos se pudo corroborar el robo de información y el modo de operar que solo encabeza las características, de los métodos y armas empleadas para llevar a cabo el crimen.

El ataque cibernético a Sony Pictures, fue uno sin precedentes el cual dejó pérdidas millonarias para la empresa productora. El ataque constó de chantajes cibernéticos, robos de películas, divulgación de películas sin estreno, robo de información de personas celebres y el retiro de apoyo de varios inversionistas. La mayoría de los ataques de *phishing* fueron organizados y dirigidos con el fin de que el usuario actúe de inmediato ante el estímulo y no se detenga a analizar los riesgos. La manipulación de los sistemas por parte del atacante dejó completamente vulnerables los sistemas, la credibilidad y acreditación de la empresa fue una cuestionada.

SECCIÓN VI: INFORME DE AUDITORÍA Y PREVENCIÓN

Trasfondo, alcance y objetivos

La auditoría fue realizada durante la fecha del 25 de febrero de 2020 y 29 de febrero de 2020. Esta examinación fue basada en las normas de auditoría de tecnología de información. La auditoría fue trabajada a través de evidencia física y el análisis de evidencia. El objetivo de esta auditoría es poder identificar las vulnerabilidades que presentó el sistema de información de la empresa Sony Pictures, y cómo afecta esto a la seguridad de su información. Se pretende realizar un **examen** de los procesos y de las actividades de la empresa, para confirmar si se rigen por las leyes y normas aplicables. Este informe contiene tres (3) hallazgos críticos.

Hallazgos detallados y recomendaciones

Hallazgo 1- Falta de *Software* antispam (*Phishing*)

Condición- La evidencia del caso demostró que a través del uso de *phishing* se lograba acceso a las computadoras de los empleados de SPE.

Criterio- Tener filtros que regulen la entrada de correos electrónicos y los empleados no deben acceder a páginas o enlaces desconocidos.

Causa- Falta de control interno.

Efecto- Acceso al sistema operativo, instalación de programas malignos y acceso a información clasificada.

Recomendación- Establecer filtros activos de correo, haciendo uso de políticas que regule la entrada de correos electrónicos externos.

Hallazgo 2: Falla en la política de datos de navegación

Condición- A través de acceso remoto a las computadoras de Sony, se lograba acceder a páginas de internet donde se descargaban *malware* para poner el sistema operativo de las computadoras completamente vulnerables.

Criterio – No permitir el acceso sin restricción a páginas no autorizadas.

Causa- Falla en los controles internos.

Efecto- Robo de información.

Recomendaciones- Instalar cookies para la protección de los datos, esto restringe contenido estableciendo al usuario seguridad y el requerimiento de autenticación.

Hallazgo 3– Falta de actualizaciones y escaso monitoreo al consumo de data de los servidores.

Condición- No hay actividad de actualización en el *software*. El sistema no contaba con las versiones y nuevos estándares de políticas y seguridad.

Criterio – Con actualizaciones que el sistema requiere, garantiza la seguridad de información y no permite que se filtre información tan fácilmente. Este control influye completamente en el desempeño del sistema y en su seguridad.

Causa- Instalación de programas malignos (gusano), que causó daños a las computadoras de Sony que fueran afectadas por virus que se replicaron en la mayoría de sus computadoras.

Efecto- Ausencia del control interno.

Recomendaciones- Actualización de los programas cada vez que sea requerido y establecer parches de seguridad, ya que esto ayuda al funcionamiento óptimo, repara las fallas y los errores de vulnerabilidad que se presenten en el sistema.

SECCIÓN VII: CONCLUSIÓN

Sony Pictures Entertainment Inc., como ya hemos investigado, es una casa productora de películas y eventos que, en noviembre del 2014, comenzó a recibir amenazas y un sin número de ataques cibernéticos por parte de un pirata informático. La investigación señala que el Sr. Park Jin es el principal sospechoso de las pérdidas millonarias que sufrió la empresa, el robo de datos a través de *phishing*, publicaciones de películas que aún no estaban en estreno y la divulgación de mas de 12,000 correos electrónicos realizados por parte de los funcionarios de SPE.

Toda la evidencia apunta a que el Sr. Park Jin, es el autor de todos los hechos que se describen en este informe contra la empresa SPE. Supo cómo realizar su intromisión al sistema haciendo uso de programas malignos para conocer sus vulnerabilidades, lograr acceder y obtener toda información deseada. Una empresa tan competitiva, que posee enemigos y con gran poder económico debería tomar en consideración más medidas preventivas que ayuden a la detección de estos delitos.

Realizar la investigación y análisis de este caso no fue una tarea fácil ya que es un caso de alto contenido. Pero es sumamente interesante conocer como los delitos cibernéticos pueden afectarnos, y el daño causado puede ser irreversible. Hoy en día numerosas entidades recopilan y almacenan información personal de sus clientes y sin contar las que exponemos en las redes sociales y en nuestros dispositivos. Es importante instruirse y aprender a conocer de lo que estamos expuesto a diario. No solo están los ciber atacantes, también las redes sociales y el internet es un medio frecuentemente utilizado para la pornografía infantil y las estafas. El internet es un medio que nos facilita y brinda acceso en nuestras tareas cotidianas, pero no debemos depositar toda nuestra confianza en ello.

SECCIÓN VIII: REFERENCIAS

- AO Kaspersky Lab. (08 de agosto de 2019). *SECURELIST*. El spam y el phishing en el segundo trimestre 2019: <https://securelist.lat/spam-and-phishing-in-q2-2019/89423/>
- AVAST Software s.r.o. (2015). *Ransomware*. <https://www.avast.com/es-es/c-ransomware>
- Crespo, S. (17 de mayo de 2019). La era de la informática está aquí y trae consecuencias.
- Cyber Security . (16 de diciembre de 2019). *Estos son los cibercriminales más buscados del mundo*. <https://cybersecuritynews.es/estos-son-los-cibercriminales-mas-buscados-del-mundo/>
- Departamento de Justicia . (21 de enero de 2020). *Departamento de Justicia de los Estados Unidos*. <https://www.justice.gov/archives/jm/criminal-resource-manual-923-18-usc-371-conspiracy-defraud-us>
- Departamento de Justicia. (21 de enero de 2020). *Departamento de Justicia de los Estados Unidos* . 1020. 18 U.S.C. § 1030—Pre October 1996: <https://www.justice.gov/archives/jm/criminal-resource-manual-1020-18-usc-1030-pre-october-1996>
- Digital Security. (24 de septiembre de 2019). *Andrei Tyurin, el ruso que se atrevió a hackear a JP Morgan Chase*. <https://www.itdigitalsecurity.es/actualidad/2019/09/andrei-tyurin-el-ruso-que-se-atrevio-a-hackear-a-jp-morgan-chase>
- Dirección de Protección de Datos. (22 de febrero de 2012). *Phishing: ataques y realidades*. HABEAS DATA: <https://habeasdatacpdp.wordpress.com/2011/02/22/phishing-ataques-y-realidades-2>
- Hispasec. (2018 de septiembre de 7). *Una al día*. Acusado un espía de Corea del Norte por el ataque a Sony Pictures y el gusano WannaCry 2.0: <https://unaaldia.hispasec.com/2018/09/acusado-un-espia-de-corea-del-norte-por-el-ataque-a-sony-pictures-y-el-gusano-wannacry-2-0.html>
- Jaimovich, D. (12 de mayo de 2018). *Infobae* . Cómo surgió y se propagó WannaCry, uno de los ciberataques más grandes de la historia: <https://www.infobae.com/america/tecno/2018/05/12/como-surgio-y-se-propago-wannacry-uno-de-los-ciberataques-mas-grandes-de-la-historia/>
- Justicia US Law. (2012). *MAIL FRAUD AND OTHER FRAUD OFFENSES - 18 U.S.C. § 1349 (2012)*. <https://law.justia.com/codes/us/2012/title-18/part-i/chapter-63/section-1349/>
- Merlatm . (2017). *Monografias.com*. Hackers - Monografias.com : <https://www.monografias.com/trabajos/hackers/hackers.shtml>
- Meyers, R. (3 de octubre de 2014). *JPMorgan: 76 millones de hogares expuestos tras 'hackeo'*. <https://www.cnet.com/es/noticias/jpmorgan-hackeo-millones-expuestos/>
- Proteger mi PC. (23 de agosto de 2018). *OsForensics, una potente herramienta de informática forense para Windows*. <https://protegermipc.net/2018/08/23/osforensics-herramienta-informatica-forense-windows/>

Rojas, E. (31 de marzo de 2014). *My Seguridad.net*. Hackers, los piratas del siglo XXI:
<https://www.muysseguridad.net/2014/03/31/hackers-piratas/>

Technology INT. (s.f.). *Forensic Toolkit (FTK)*. <http://technoint.weebly.com/software-de-anaacutelisis-informaacutetico-forensic-tool-kit-ftk.html>