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

Esquema de Fraude en la Bolsa de Valores

Análisis del caso: U.S.A. vs. VADYM IERMOLOVYCH

Caso#:16-CR-00235

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Especialidad en Seguridad de Información e Investigación de Fraude

Febrero 2020

Preparado por:

Luis A. Rolón Torres

Sirva la presente para certificar que el Proyecto de Investigación titulado

Esquema de Fraude en la Bolsa de Valores

Análisis del caso: U.S.A. vs. VADYM IERMOLOVYCH

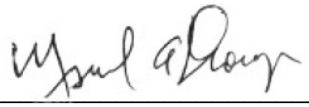
Caso#:16-CR-00235

Preparado por:

Luis A. Rolón Torres

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

Febrero 2020



Miguel A. Drouyn Marrero, Profesor

Agradecimientos

Aprovecho este espacio para agradecer a mi esposa e hijas por todo su apoyo tan especial en todo este proceso. Ellas forman una parte muy importante en mi vida. Espero, a través de mis acciones, poder servirles de ejemplo para que ellas puedan alcanzar sus sueños también.

A todos mis compañeros les agradezco su apoyo incondicional y el poder compartir juntos esta aventura única en nuestras vidas. No podría dejar atrás aquellos profesores que de una forma u otra han influenciado positivamente en mi aprendizaje y desarrollo profesional. A todos ustedes que día a día tuvieron la paciencia de poner su mejor cara en los momentos difíciles. ¡Gracias!

Hay tantas personas a las cuales quisiera agradecer, sin embargo, no me llegan las palabras. Solo me resta decirles a todos muchas gracias por brindarme la oportunidad de aprender junto a ustedes.

Agradezco al Dr. Miguel Drouyn por aceptarme en el programa de maestría y a todos los otros profesores por todo lo que aprendí durante sus cursos.

Tabla de contenido

Tabla de Figuras

SECCIÓN1: INTRODUCCIÓN Y TRASFONDO

Introducción

De acuerdo con Legal Information Institute from Cornell University Law School (s.f.), se considera fraude cibernético e informático aquel que ha sido cometido a través de la utilización de una computadora o medio tecnológico y el internet. Los fraudes cibernéticos pueden ser elaborados por uno o varios individuos, aunque generalmente es más común a través de la participación de múltiples individuos. Estos suelen utilizar herramientas muy particulares, tales como *nmap, Exploit Database, John the Ripper, THC-Hydra, Metasploit* y otros, para obtener información e identificar vulnerabilidades antes de realizar sus ataques cibernéticos.

Según nos indica la página cibernética Data Connectors (s.f.), alrededor de 43% de las empresas en los Estados Unidos han sido víctimas de algún ataque cibernético ocasionando pérdidas millonarias reportado durante el 2018. Uno de los casos mencionados como ejemplo es el estado de California que tuvo pérdidas de $214 millones relacionado a estos ataques. Lo que demuestra claramente el aumento de esta modalidad según pasan los años. Ciertamente, ver estos datos nos lleva a pensar que existe una gran necesidad de orientar a la población en cómo prevenir ataques cibernéticos y en particular a las grandes empresas. En adición se debe desarrollar acciones concretas para mitigar este tipo de modalidad a la cual todos estamos expuesto.

A pesar de los esfuerzos del gobierno de Estados Unidos y de autoridades locales por proteger a los ciudadanos y a las empresas de este tipo de ataques, continuamos viendo con mayor frecuencia diversas formas o maneras de ataques cibernéticos y actos fraudulentos. Podemos tomar como ejemplo el caso USA v. Vadym Iermolovych (2016), en el cual el joven de

28 años de nombre Vadym Iermolovych junto a otros individuos de descendencia ucraniana atacaron varias empresas con el propósito de beneficiarse económicamente. Estos jóvenes utilizando métodos específicos atacaron varias empresas adquiriendo información confidencial y sensible de diferentes empresas que no habían sido públicamente expuestos. La información obtenida luego fue vendida a unos inversionistas que aprovechando la ventaja de tener la información antes que sus competidores lograron generar beneficios monetarios de sobre 30 millones de dólares. A continuación, se describe el caso en más detalles.

Descripción del caso

Número de caso ***2:16-CR-00235***

Acusado

Figure 1 - Vadym Iermolovych (obtenido de facebook, 2013)

Vadym Iermolovych,
a/k/a "Vadim Ermolovich",
a/k/a "Dima Ermolovich",
a/k/a "Dim", a/k/a "Dima",
a/k/a "Dingos777",
a/k/a "Vaer",
a/k/a "Nadal",
a/k/a "PriestTF"
and a/k/a "Kamazik".

Coacusados:

Ivan Turchynov,

a/k/a “Ivan Turchinov”,

a/k/a “Ivan Turchinoff”,

a/k/a “Vladimir Gopienko”,

a/k/a “DSU” y Oleksandr Ieremenko,

a/k/a “Aleksandr Eremenko”,

a/k/a “Zlom”,

a/k/a “Lamarez”.

Víctimas

Las víctimas en el caso fueron las empresas Marketwired L.P, PR Newswire Association LLC (PRN) y Business Wire.

Investigadores

Las investigaciones estuvieron a cargo de Jeh Johnnson, Secretario de Seguridad Nacional de los Estados Unidos; Joseph P. Clancy Director del servicio secreto de los Estados Unidos; Diego Rodríguez Subdirector del FBI a cargo; Oficina de campo de Nueva York y la presidenta de la Comisión de Bolsa de Valores de los Estados Unidos (SEC), Mary Jo White y Agentes especiales de la Oficina de Campo de Newark, bajo la dirección del Agente Especial Interino a Cargo Jeffrey Wood.

Abogados de la defensa

La representación legal por parte del acusado (Vadym Iermolovych) fue a través del licenciado K. Anthony Thomas, Esq.

Fiscales

Los fiscales del ministerio público fueron representados por Andrew S. Pak y Daniel Shapiro, fiscales adjuntos de la Unidad de delitos económicos, Sección de piratería informática y propiedad intelectual, David M. Eskew, Jefe adjunto de la Unidad de delitos generales, Fiscal adjunto Svetlana M. Eisenberg, de la Unidad de delitos generales, y La fiscal federal adjunta Sarah Devlin de la Unidad de Decomiso de Activos y Lavado de Dinero.

Juez (a)

El caso que se presenta fue presidido por la Honorable Madeline Cox Arleo, Juez de Distrito de los Estados Unidos para el Distrito de Nueva Jersey.

Trasfondo

De acuerdo a USA v. Vadym Iermolovych (2016), el acusado natural de Ucrania obtuvo acceso no autorizado a computadoras y servidores de las empresas Maketwired L.P. (marketwired), PR Newswire Association LLC (PRN) y Business Wire con el propósito de vender información y lucrarse económicamente. Este junto a otros conspiradores robó información confidencial la que posteriormente vendió a inversionistas en los Estados Unidos. Los inversionistas utilizaron la información adquirida para realizar inversiones.

Esto se pudo conseguir utilizando diversos mecanismos de ataques para poder perpetrar en los sistemas de información de las empresas víctimas. Algunos de estos ataques fueron a través de *SQL Injection, Bruce force attacks, malware* y *reverse shells malwares*. Estos ataques fueron realizados por varios años logrando ganancias de sobre 30 millones de dólares.

Descripción de hechos

Para febrero del 2010, Vadym Iermolovych junto a otros co-conspiradores realizó una serie de ataques contra la empresa Marketwired utilizando el de SQL Injection como mecanismo para obtener acceso no autorizado a sus servidores. Entre el 24 de abril y el 20 de julio del 2012 uno de los co-conspiradores (Turchynov) envió alrededor de 390 ataques a dicha empresa.

El 26 de febrero de 2010 ocurrió el primer robo de información a la empresa Marketwired. Luego de haber obtenido acceso no autorizado a los servidores Vadym Iermolovych instaló múltiples *malware* o *reverse shells* con el propósito de hacer mucho más fácil el robo de la información. El método de *reverse Shells* le permitía establecer conexiones sin ser detectado permitiéndole estar más tiempo realizando los robos de documentos.

Para marzo de 2012 Vadym Iermolovych obtuvo información de empleados y contactos que permitieron la entrada a la red de la empresa Marketwired. De esta manera obtuvo acceso a más de 100,000 documentos con información valiosa para las inversiones en la bolsa de valores. Para ese entonces la información todavía no era de dominio público. Este tipo de robo continuó hasta finales de julio de 2015.

Por otro lado, la empresa PRN, fue víctima en tres ocasiones de Vadym Iermolovych. Desde julio de 2010 a enero de 2011 fue la primera vez que se tuvo acceso no autorizado a los servidores de la empresa PRN. En una segunda ocasión para julio 2011 a marzo 2012 y finalmente entre enero a marzo de 2013. Durante este periodo Vadym Iermolovych logro acceder a información de informes no publicados relacionados al mercado de valores. Pudo obtener acceso a sobre 40,000 documentos aproximadamente.

Para el 12 de enero de 2011 la empresa PRN realizó unas mejoras en su infraestructura el cual ayudo a mantener fuera a Vadym Iermolovych y otros co-conspiradores. No obstante, al no poder tener acceso a PRN enfocaron sus ataques con mayor énfasis en la empresa Marketwired. Para julio de 2011 a marzo de 2012 Vadym Iermolovych y otros co-conspiradores lograron acceso a la red de PRN instalando luego en sus servidores un *malware* que les ayudó a poder mantener el acceso a estos.

Luego de varios meses PRN logró identificar y remover el *malware* que se había instalado en los servidores logrando eliminar el acceso de los *hackers* por segunda ocasión. Sin embargo, entre enero y marzo de 2013, Vadym Iermolovych, logra nuevamente tener acceso a los servidores. En esta ocasión para poder infiltrarse en la red de PRN tuvieron que comprar una gran base de datos de credenciales robados obtenidos de una filtración a las redes sociales. Utilizaron la información de la base de datos para localizar posibles empleados de PRN y de esta manera utilizar credenciales para infiltrarse en la empresa.

A principios de marzo de 2013 la empresa PRN volvió a detectar y a bloquear la filtración de Vadym Iermolovych en su red. Al no poder infiltrarse en la red de PRN volvió a enfocarse con mayor intensidad en la empresa Marketwired en la cual mantenían acceso.

Entre marzo a junio de 2012 pudieron acceder en los sistemas de otra de las víctimas conocida como Business Wire. El Conspirador Vadym Iermolovych compró a otro *hacker* una base de datos que tenía credenciales de los empleados de Business Wire. Estas credenciales se obtuvieron por un *hacker* que utilizando el método de *SQL Injection* pudo acceder exitosamente la red interna de Business Wire.

Acusaciones, cargos y penalidades

El Departamento de Justicia de los Estados Unidos entregó a principios de noviembre de 2015 un documento de aceptación de culpabilidad al abogado del acusado el Sr. K. Anthony Thomas. El mismo fue firmado por el acusado y su abogado el 14 de noviembre de 2015 aceptando la culpabilidad de haber cometido los delitos de lo cual se le acusaba. Los cargos descritos en el documento son:

Cargo uno

18 U.S. Code § 1349, Conspiración para cometer fraude electrónico

18 U.S. Code § 1343, Conspiración para cometer fraude electrónico

Cargo dos

18 U.S. Code § 1030(a) (2), Conspiración para cometer fraude y actividades relacionadas en conexión con computadoras

Cargo tres

18 USC § 1028A (c), Robo de identidad agravado

18 USC § 1028A (a) (1), Robo de identidad agravado

El acusado enfrenta una sentencia al cargo uno por la violación del *18 U.S. Code § 1349,* del cual Vadym Iermolovych hace la declaración de culpabilidad, de 20 años de prisión y una multa máxima o igual a la más alta de: (1) 250,000 dólares, o (2) el doble de la ganancia pecuniaria que cualquier persona derivada o (3) el doble de la cantidad bruta de cualquier pérdida en dinero sufrida por las víctimas del delito.

Para el cargo dos por la violación al código *18 U.S. Code § 371* enfrenta una penalidad máxima de 5 años de prisión. En adición una fianza máxima de (1) 250,000 dólares, o (2) el doble de la ganancia que cualquier persona derivada o (3) el doble de la cantidad bruta de cualquier pérdida monetaria sufrida por las víctimas del delito.

En relación al cargo tres de la sentencia por violación al código *18 USC § 1028A* llevara una pena mandatorio de dos años de prisión. La misma no podrá correr de forma consecuente a otras sentencias contrario a los cargos uno y dos que sí pueden correr consecutivamente.

A pesar que las sentencias han sido en referencia al United States Sentencing Commission, Guidelines Manual (2015) este no implica que la sentencia final será tal como se describe en dicha guía. La sentencia final será impuesta por el Juez(a) que estará a cargo del caso.

Definición de términos

Reverse shells: es un tipo específico de *malware* diseñado para inicializar una conexión desde una computadora a otra desde la computadora infectada con este *virus* o *malware*. (Acunetix, 2019)

Brute Force Attacks: es un mecanismo en el cual se busca adivinar la identidad de una cuenta para lograr entrar a los sistemas de información previamente identificados para atacar. Se utiliza un diccionario de posibles valores y una herramienta para realizar el proceso de intentar adivinar el mismo. (Sophos.com, s.f.)

***Internet Protocol (IP) address**:* es una numeración única asignada a cada conexión en el internet. Cada equipo o dispositivo de red se le asigna una numeración IP para que pueda transmitir o recibir datos a través de la comunicación entre uno o varios dispositivos de red. (Cisco.com, 2016)

***Malware**:* son programas diseñados con el único propósito de afectar a un tercero con propósito de dañar, alterar o extraer datos. Estos suelen propagarse a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del *malware* peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías. (Cisco.com, s.f.)

Structured Query Language (SQL): es un lenguaje de programación diseñado para manejar, extraer o editar datos de sistemas de almacenamiento de datos relacionados. (TechTarget, s.f.)

SQL Injection Attacks: es una técnica donde los usuarios malintencionados pueden inyectar comandos *SQL* en una sentencia *SQL*, a través de la entrada de la página web.

Los comandos *SQL* inyectados pueden alterar la sentencia *SQL* y comprometer la seguridad de una aplicación web permitiendo acceso remoto a la aplicación y luego a las bases de datos. Algunos ejemplos de estos ataques en páginas web donde se solicita contraseña y código de usuario seria: (OWASP, s.f.)

```
$username = 1' or '1' = '1
$password = 1' or '1' = '1

SELECT * FROM Users WHERE Username='1' OR '1' = '1' AND Password='1' OR
'1' = '1'
```

Hackers: se refiere a una o más personas que utilizando sus conocimientos en el campo de la informática buscan como principio alterar, extraer, comprometer o destruir información de un tercero de forma no autorizada. Generalmente, este tipo de sujetos utilizan programas específicos diseñados para esos propósitos. Estos pueden ser identificados bajo uno de los siguientes:

> ***Black Hat***: los *hackers* de sombrero negro, como se les conoce, son aquellos que buscan la explotación de potenciales fallas de seguridad cibernética. Contrario a los de sombrero blanco estos buscan alterar, borrar o robar información de forma ilícita para satisfacer sus necesidades o para su propio beneficio. Atacan a las empresas con la utilización de virus, *malware* y otros mecanismos.
>
> ***Grey Hat***: los *hackers* a los que se le denomina de sombrero gris suelen identificar las vulnerabilidades o fallas en los controles de seguridad cibernética, pero a diferencia de los de sombrero blanco quienes hacen público las fallas, estos podrían negociar con el gobierno u otros la información de las fallas.
>
> ***White Hat***: los denominados como *hackers* de sombrero blanco son aquellos que por lo general identifican potenciales vulnerabilidades y los hacen públicos con el propósito de que se puedan corregir. Éstos, en su mayoría son contratados por las empresas para realizar ejercicios de identificación de estas vulnerabilidades. A pesar de encontrar los fallos no se procede a realizar daño alguno. (Wikipedia.org, s.f.)

PHP Script: es un lenguaje de *scripting* que opera en el lado del servidor. Está diseñado para el desarrollo web, pero también se utiliza como un lenguaje de programación de propósito general. Un *script php* no autorizado es un programa que puede ejecutarse sin ser detectado dentro de un servidor comprometido por los *hackers*. (Tutorialspoint.com, s.f.)

Password Hashes: son cadenas de datos cifradas generados cuando se pasa una contraseña a través de un algoritmo de cifrado. Las contraseñas de las cuentas de red a menudo se almacenan en la red como un *hash* de contraseña como medida de seguridad. (Oracle.com, s.f.)

Nmap: la aplicación de *nmap* (*network mapper*) tiene como funcionalidad principal realizar un descubrimiento de una red o redes. En adición sirve como utilidad para auditar la red o *network* en una empresa. Es totalmente libre de costo bajo la licencia de *open source*. Es comúnmente utilizada por administradores de redes para realizar inventario de *IP Address* activas en la red. Es una aplicación muy flexible que permite realizar un escaneo de la red a un IP o un rango de IPs. Tiene versiones para sistemas Linux, Mac OS X y Windows (*Zenmap*). (Nmap.org, s.f.)

John the Ripper: es un aplicativo diseñado para detectar contraseñas débiles o fáciles y descifrar las mismas. El mismo está disponible en diferentes versiones de sistemas operativos tales como Unix, Windows, DOS, OpenVMS y otros. Este sistema utiliza varios mecanismos de cifrado para revelar la contraseña en forma legible. Algunos de estos métodos son encontrados en varios sistemas Unix, *Kerberos/AFS* y *Windows LM hashes*. Su utilización y efectividad están basados en usar una lista o diccionario de contraseñas combinados con comandos y opciones que indican al comando que hacer. Un ejemplo de su utilización sería algo como ***John - -wordlist=password.lst - -rules passwd***. las opciones a utilizarse podrían variar dependiendo del sistema operativo en el cual se ejecuta. (OpenWall.com, s.f.)

OSForensic: es una herramienta forense utilizada para descubrir, identificar y administrar evidencia digital que se encuentra en los sistemas informáticos y dispositivos de almacenamiento digital. *OSForensics* cuenta con una variedad de módulos para simplificar la tarea de analizar la gran cantidad de datos sobre sistemas en vivo y almacenamiento medios con una interfaz fácil de usar. Estos módulos incluyen uno de búsqueda por nombre de archivo que se puede identificar

material que podría servir de evidencia. En adición, incluye otros módulos más sofisticados de análisis. (PassMark Software, s.f.)

Vishing: la actividad de ingeniería social a través del sistema telefónico, la mayoría de las veces utiliza funciones facilitadas por *VoIP* (voz sobre Internet Protocol), para obtener acceso no autorizado a datos confidenciales. (Malwarebytes.com, s.f.)

Smishing: es similar a "*vishing*", pero utilizan la ingeniería social a través de un mensaje de texto. (Malwarebytes.com, s.f.)

PII (Personally Identifiable Information): significa información que se puede usar para distinguir o rastrear la identidad de un individuo, ya sea solo o cuando se combina con otra información personal o de identificación que está vinculada o vinculable a una persona específica. Parte de la información que se considera PII está disponible en fuentes públicas, como guías telefónicas, sitios web públicos y listados de universidades. Este tipo de información se considera PII pública e incluye, por ejemplo, nombre y apellido, dirección, número de teléfono del trabajo, dirección de correo electrónico, número de teléfono del hogar y credenciales educativas generales. La definición de PII no está anclada a ninguna categoría de información o tecnología. Más bien, requiere una evaluación caso por caso del riesgo específico de que un individuo pueda ser identificado. La no-PII puede convertirse en PII siempre que la información adicional se haga pública, en cualquier medio y de cualquier fuente, que cuando se combina con otra información disponible, se pueda usar para identificar a una persona. (Legal Information Institute, s.f.)

SECCIÓN 2: REVISIÓN DE LITERATURA

Introducción

La tecnología relacionada con los sistemas de información y las comunicaciones han ido evolucionando de una manera exponencial permitiendo que hoy se puedan ejecutar ciertas tareas de una manera distinta a como se hacía en décadas pasadas. Paralelo al avance de la tecnología se puede observar un aumento en la dependencia al uso de equipos y dispositivos de computación que son adquiridos por las empresas para facilitar la producción y garantizar la eficiencia de sus funciones, así como un incremento de la influencia de estos equipos en asuntos de la vida cotidiana. Lo que en otros tiempos se hacía manual, hoy se realiza con una mayor rapidez gracias al uso de los equipos y los sistemas de procesamiento de datos. Esta dependencia a la tecnología se da en diferentes contextos, como el área industrial, el área de producción científica, el sector académico, entre otros. Este fenómeno es algo que se puede observar a nivel mundial sobre todo en aquellos países que cuentan con un mayor desarrollo económico.

Así como la tecnología ha traído unos beneficios para el desarrollo económico y científico en los países, también se ha dado el nacimiento de unos comportamientos y acciones que atentan contra el orden y el funcionamiento de las instituciones sociales que están establecidas. La era de la información y el conocimiento no está ajenas de acciones que pueden ser consideradas antiéticas y delictivas. Debemos reconocer que el siglo XXI ha estado caracterizando por grandes progresos a nivel de los sistemas de información y de las comunicaciones. Se han desarrollados equipos de computadoras más eficientes donde hay mayor capacidad de almacenamiento y procesamiento de la información. La humanidad ha sido testigo como “chips” instalados en las computadoras y otros equipos se han achicado de maneras

inimaginables sin dejar de perder funcionalidad, sino que, por el contrario, esos dispositivos en miniaturas son capaces de una mayor eficiencia y almacenamiento de datos.

El progreso ha estado acompaño de nuevos problemas y grandes retos. La sociedad de hoy debe hacer frente a las vulnerabilidades que conlleva un mundo hiperconectado donde el internet es un elemento crucial para acceder y compartir información. Es más común hoy escuchar que se habla de términos como: crímenes o delitos cibernéticos, guerra cibernética, terrorismo cibernético, entre otros. No todo se presenta como positivo en el desarrollo de la tecnología, pues el uso de la Red favorece el surgimiento de estos problemas a los que la sociedad debe hacer frente y donde los ciudadanos tienen que aprender a convivir con la nueva realidad, por la frecuencia en la que surgen noticias acerca de un hecho ilícito que se ha producido en la Red (Sánchez, 2012). Tal y como plantea Hernández (2009) "la extensión del uso de los ordenadores y de las redes de transmisión de datos en la mayoría de los ámbitos de nuestra sociedad, todos y prácticamente todos los delitos pueden cometerse a través de sistemas informáticos; en este sentido, las conductas ilícitas vinculadas con los sistemas informáticos son muchas y heterogéneas".

Los distintos delitos que se pueden dar a través del internet es algo que preocupa no solo a las empresas, las diversas organizaciones, los gobiernos y los individuos. Por ejemplo, en algunos de los países sus preocupaciones han sido llevadas en foros internacionales como es el caso de la Organización de las Naciones Unidas (ONU). En el año 2010, los países miembros de la ONU aprobaron la Resolución 65/230 para que la Comisión de Prevención del Delito y Justicia Penal llevara a cabo un estudio exhaustivo sobre los delitos cibernéticos. Para realizar el estudio se convocó un grupo intergubernamental de expertos para que no solo examinaran los delitos que se están llevando a través de la internet, sino que se recopilara información sobre la

respuesta que están dando los países para reducir la incidencia de estos crímenes. El grupo de experto en sus deliberaciones indicó que el delito cibernético iba en aumento y aunque se podía considerar como un problema universal no necesariamente era un fenómeno uniforme en los países. Algunos expertos señalaron incluso la complejidad de las formas de delincuencia y el peligro que representaba para el desarrollo de los países. Enfatizaron en los aspectos de carácter transnacional de las redes de computadoras y los delitos que se cometen. A su vez plantearon la necesidad de una respuesta oportuna para lograr acuerdos entre los países para que haya una mayor cooperación y respuesta concertada.

Específicamente cuando analizamos los elementos del fraude electrónico (delito específico al que atiende el caso seleccionado) vemos que comparte muchos de los elementos del fraude como delito, pero aquello que lo distingue es el medio que se utiliza para lograr el engaño con fines lucrativos. Según Gabaldón (2006), el fraude electrónico es toda conducta dirigida a la obtención de un provecho económico indebido, mediante la apropiación, la falsificación, la interferencia y la reproducción de códigos, instrucciones o programas, tanto sobre instrumentos portables como sobre programas incorporados a sistemas de procesamiento de datos, que permiten el acceso a dinero en efectivo o bienes y servicios con cargo diferido a cuentas bancarias.

Por ejemplo, en Estados Unidos se calcula que se generan perjuicios económicos, por los delitos informáticos que superan los 10,000 millones de dólares y en donde el 90% de los delitos informáticos que esta investiga el FNI tiene que ver con internet (Ramírez & Rodríguez, 2009).

De acuerdo a la página cibernética *Ambito.com (2018)* el reporte anual de fraude y riesgo de Kroll 2017/2018, realizó una encuesta mundial a ejecutivos de diferentes empresas quienes

aseguran que el fraude se encuentra en su mayor pico. De acuerdo a los resultados del informe el fraude que nos muestra la Figura 2, esta modalidad ha ido en aumento desde el 2012.

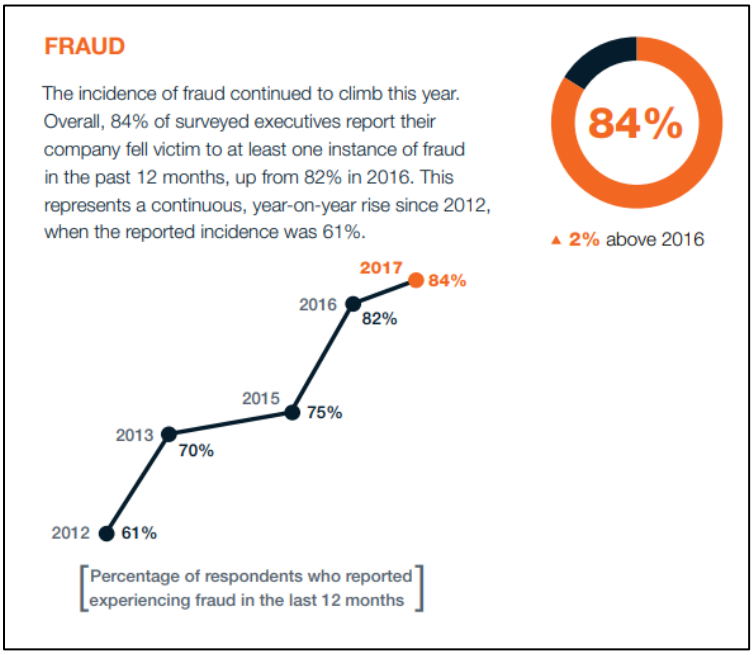


Figure 2 – Crecimiento de incidencia en Fraude electrónico (Recuperado de http://www.ambito.com/912536-empresas-sufrieron-nivel-record-de-fraude-cibernetico-en-2017)

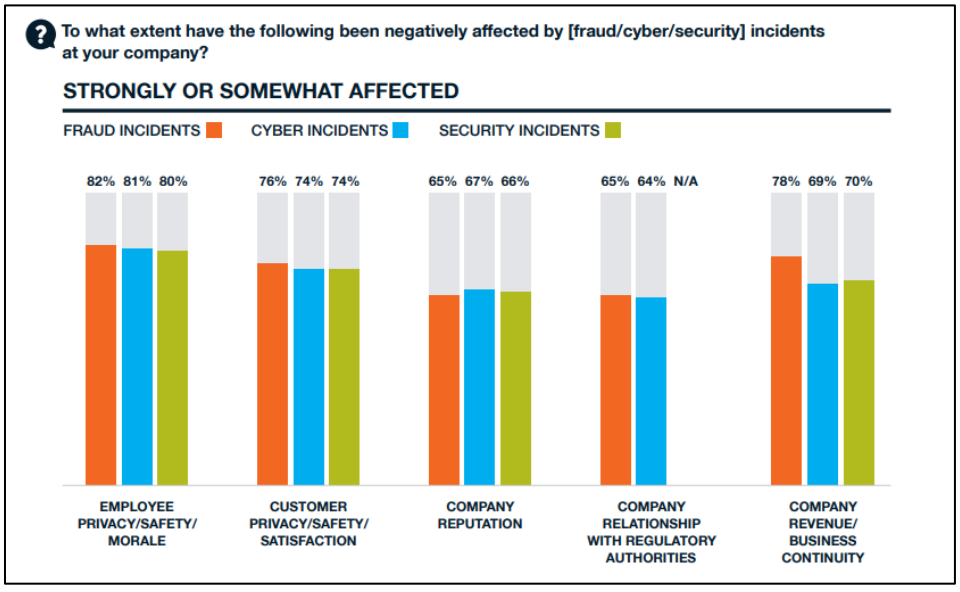


Figure 3 – Estadística de afectados por tipo (Recuperado de http://www.ambito.com/912536-empresas-sufrieron-nivel-record-de-fraude-cibernetico-en-2017)

Según unas estadísticas publicadas por la página Condusef.gob.mx (s.f.) que se muestra en la Figura 4 es otro ejemplo que muestra claramente lo vulnerables que estamos cada día.

FRAUDES CIBERNÉTICOS Y TRADICIONALES:

Al tercer trimestre de 2019, las quejas por fraudes cibernéticos crecieron 38% respecto de 2018 y representan cada año una mayor proporción.

	2015	2016	2017	2018	2019	VAR. (2019 vs 2018)
TOTALES	2,704,355	3,917,674	4,974,334	5,364,838	6,614,867	
CIBERNÉTICOS	505,141	1,253,371	2,534,834	3,162,217	4,359,807	38%
	19%	32%	51%	59%	66%	-
TRADICIONALES	2,199,096	2,660,657	2,417,101	2,192,096	2,255,048	3%
	81%	68%	49%	41%	34%	-
Por definir	118	3,646	22,399	10,525	12	-

Figure - 4 Fraudes cibernéticos tradicionales (recuperado de https://www.condusef.gob.mx/gbmx/?p=estadisticas)

Es evidente la necesidad de los gobiernos de establecer mejores políticas públicas que garanticen en cierta manera la protección de la información de los individuos o corporaciones. A pesar de los grandes esfuerzos realizados por algunos gobiernos, aún existen grandes desafíos relacionados a la cooperación entre las naciones como Rusia, por mencionar alguno para poder atacar el crimen cibernético de manera más eficiente. Según avanzamos en la creación de herramientas más inteligentes para la protección es necesario también fortalecer la legislación para este tipo de crimen.

Los casos de fraude cibernéticos no solo atacan a individuos, pero a grandes empresas como bancos y aquellas que de alguna manera u otra forman parte del mercado de valores. El mercado de valores en el cual se establece el curso económico de las empresas o naciones en general. La gran importancia de estas empresas es mantener la información confidencial en total protección antes de que ocurran las negociaciones o transacciones que determinan el curso

económico de éstas. El que la información caiga en manos no autorizadas antes de ocurrir las negociaciones podría poner en ventaja aquellos que posean dicha información.

Leyes Aplicables, *Cornell University Law School (s.f.)*

18 U.S. Code § 1349 **Intento y conspiración**

Toda persona que intente o conspire para cometer un delito bajo este capítulo estará sujeta a las mismas penas que las prescritas para el delito cuya comisión fue objeto del intento o conspiración.

18 U.S. Code § 1343 **Fraude por cable, radio o televisión**

Quienquiera que haya ideado o pretenda idear cualquier esquema o artificio para defraudar, o para obtener dinero o propiedad mediante falsas o fraudulentas pretensiones, representaciones o promesas, transmita o hace que se transmitan por medio de comunicación por cable, radio o televisión. En el comercio interestatal o extranjero, cualquier escritura, signo, señal, imagen o sonido con el fin de ejecutar tal esquema o artificio, será multado bajo este título o encarcelados no más de 20 años, o ambos. Si la infracción ocurre en relación con, o implica cualquier beneficio autorizado, transportado, transmitido, transferido, desembolsado o pagado en relación con un desastre o emergencia principal declarado presidencialmente (como se definen estos términos en la sección 102 del Robert T. Stafford (42 USC 5122)), o afecta a una institución financiera, dicha persona será multada no más de $ 1,000,000 o encarcelada no más de 30 años o ambos.

18 U.S. Code § 1030(a) (2) **Fraude y actividad relacionada en conexión con computadoras**

Cualquier individuo(a) que intencionalmente tenga acceso a una computadora sin previa autorización.

18 USC § 1028A **Robo de identidad agravado**

Quienquiera que, durante y en relación con cualquier infracción de felonía enumerada en el inciso (c), transfiera con conocimiento de causa, posea o utilice, sin autoridad legal, un medio de identificación de otra persona, además de la pena provista para tal felonía, A una pena de prisión de 2 años.

Casos relacionados

USA vs Stanislav Vitaliyevich Lisov (a/k/a "Black", a/k/a "Blackf")

En el caso *United States vs. Lisov*, (*Court Listener*, 2017), el perpetrador (Lisov) en conjunto con otros cómplices estuvieron robando dinero de diferentes maneras a sus víctimas que desconocían o no tenían el conocimiento para poder protegerse o detectar a tiempo lo ocurrido. Estos, en especial Lisov, utilizaron un *malware* conocido como *Neverquest* para infectar las máquinas. El *malware* tiene como propósito principal robar información de cuentas de usuarios, tales como: nombre de usuarios, contraseñas contestaciones de preguntas secretas específicos de cuentas de bancos. Desde junio 2012 hasta enero 2015 estuvieron realizando exitosamente el crimen cibernético. Esto se debía en parte a que Lisov mantenía la infraestructura de varios de sus víctimas y se le hacía fácil infectar las máquinas y servidores que contenían la información sensible que necesitaban.

United States v. Costea (1:15-cr-00375)

En el caso **United States v. Costea** *(Court Listener, 2015)* los perpetradores Robert Codrut Dumitrescu, Teodor Laurentiu Costea y Cosmin Draghici, desde octubre de 2011 hasta febrero de 2014 aproximadamente estuvieron robando información PII (*personally Identifiable information*) utilizando un esquema fraudulento de *vishing* y *smishing*. Como parte del esquema se utilizaron máquinas o servidores que estos infectaron instalando aplicativos de envío masivo de correos electrónicos y de manejo de llamadas y grabaciones respectivamente. Utilizando el aplicativo previamente en los servidores, el mismo comenzaba a realizar llamadas masivas y envío de texto a potenciales víctimas. Tanto el texto como la grabación tenían como enfoque el poder obtener información de las víctimas que pudiera ser utilizada para infiltrarse en sus cuentas bancarias u otros. En el caso de aquellos que recibían la llamada automatizada esta aparentaba ser de un banco en el cual se le pide actualizar información PII. Una vez la víctima introducía la información esta era guardada en los servidores para ser utilizada luego. En el caso de los mensajes de texto (*Smishing*) es bien parecido al de *Vishing,* pero la víctima en vez de utilizar su voz lo envía a través de su celular o equipo móvil. La información adquirida a través de este esquema tenía un valor aproximado de $21,000,000.

Herramientas de investigación

La detección del fraude electrónico cada día depende más de herramientas sofisticadas y de personal debidamente capacitado en tales herramientas y en tecnología en general. Para poder mitigar posibles brechas de seguridad las empresas deben implementar políticas corporativas, y equipos como *firewalls*, *IPS* (*Intrusion Prevention System), DLP (Data Loss Protection System), SIEM*, *Antivirus, Webfiltering, AntiSpaming, Phishing detection,* entre otros. Estos mecanismos o

controles ayudan de forma proactiva a minimizar las incidencias, pero hay que tener siempre en mente que existirá un margen de vulnerabilidad.

Una de las herramientas que se podría utilizar eficientemente para la detección de posibles brechas de seguridad es el *SIEM (Security Information and Event Management)*. Estos sistemas tienen como funcionalidad principal colectar todo tipo de evento generado por los diferentes tipos de herramientas o aplicaciones y a su vez crear una correlación de eventos que apunten a un potencial ataque cibernético. A pesar de que los sistemas SIEM pudiera ser muy efectivo en identificar potenciales brechas de seguridad esto solo sirve de método informativo. Por otro lado, aunque hay muchas herramientas y controles muy efectivos los *firewalls* y los *antivirus* siguen siendo los de mayor protección, ya que son el punto céntrico por donde pasa toda la información de las empresas y en el caso de los equipos como laptops o Tablet son protegidos de malware.

SECCIÓN 3: SIMULACIÓN

A continuación se presenta de forma simple y visual como Vadym Iermolovych realizaba su operación fraudulenta contra PRN. La simulación es una representación personalizada y no necesariamente representa en detalle los hechos reales del caso. El propósito principal es poder presentar el esquema del fraude de una manera simple.

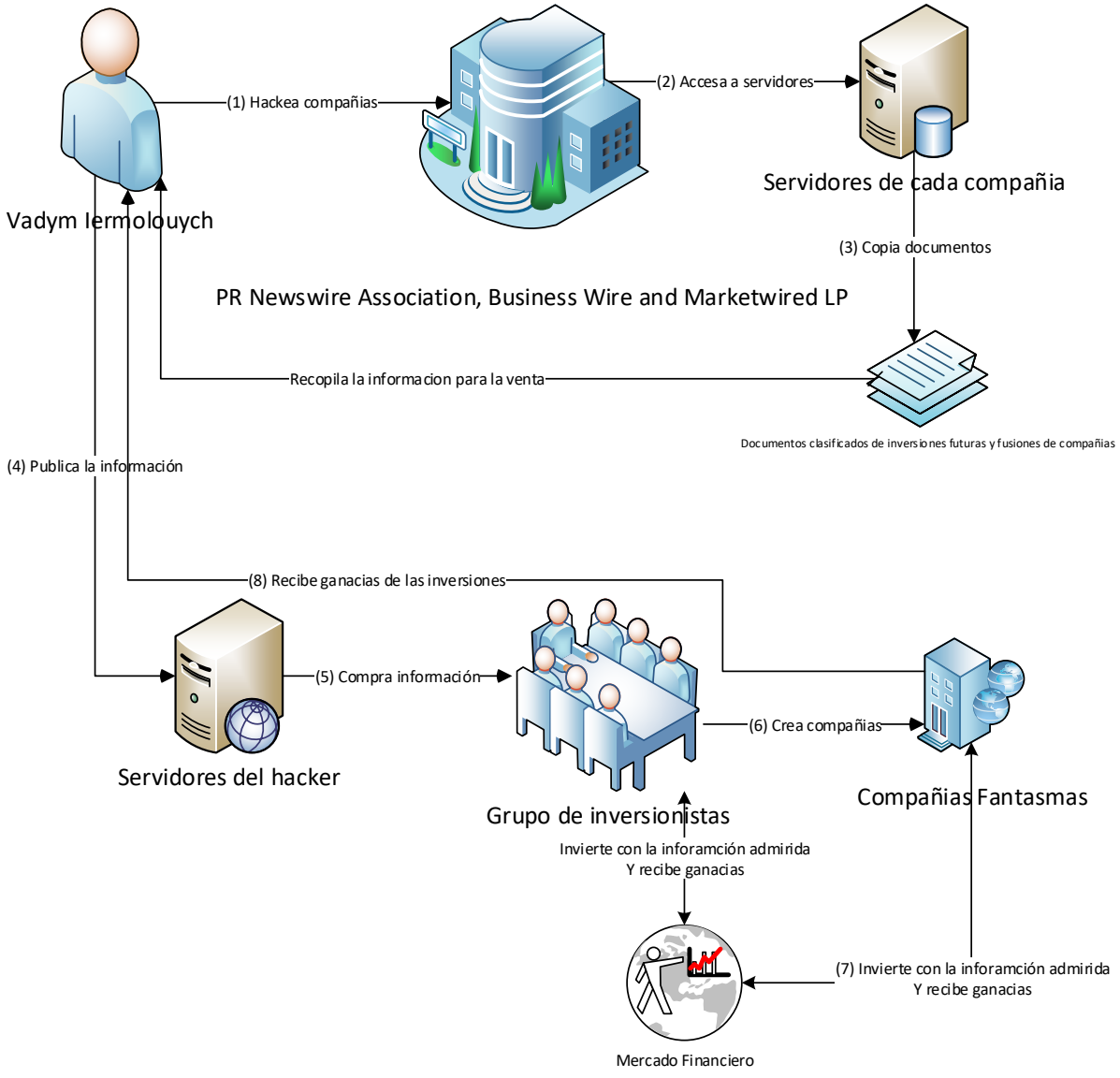


Figure 5 - Esquema del Fraude

A continuación, se desglosan los pasos utilizados por el perpetrador mostrados en la gráfica (figura 5).

1) Utilizando diversas herramientas, tales como *nmap*, Vadym Iermolovych estuvo recopilando información de las empresas PRN (víctima) utilizando el internet para obtener detalles de su ubicación, tipo de servicios que brindan, IP externo, dominio entre otros detalles.

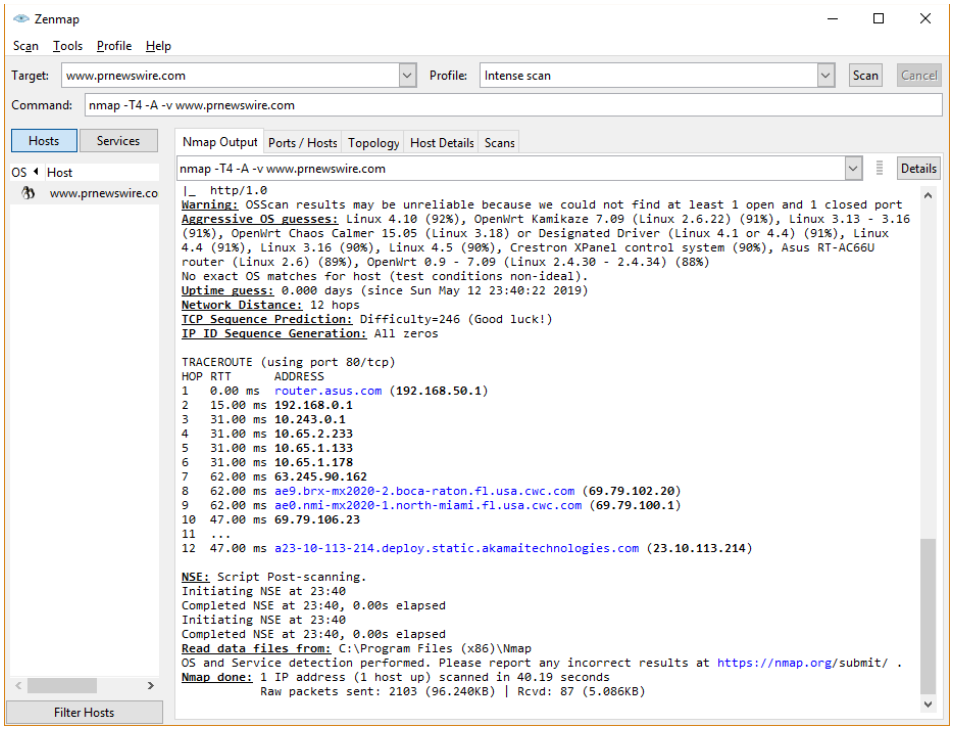


Figure 6 - Zenmap Tool

2) Luego de haber obtenido los servicios y puertos abiertos de los servidores de PRN procedió a explotar las vulnerabilidades en servidores de *SQL*. Este realizó un ataque de *SQL injection* para adquirir acceso a la base de datos donde estaba la información de la empresa.

3) Luego de obtener acceso a la información este procedió a copiar a su servidor los datos y documentos con información confidencial. Gran parte de los datos e información adquiridos eran publicaciones aun no expuestas al público en generar de inversiones, negocios nuevos o compra de empresas entre otros.

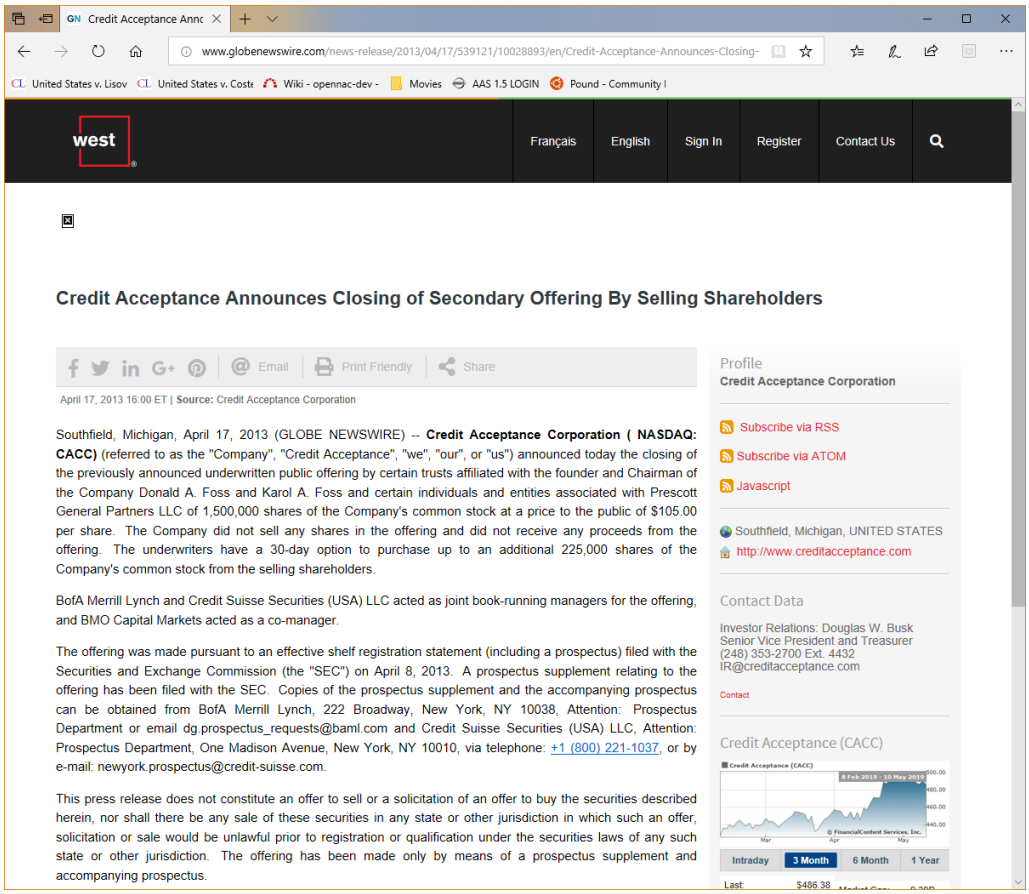


Figure 7 - obtenido de http://www.globenewswire.com/news-release/2013/04/17/539121/10028893/en/Credit-Acceptance-Announces-Closing-of-Secondary-Offering-By-Selling-Shareholders.html

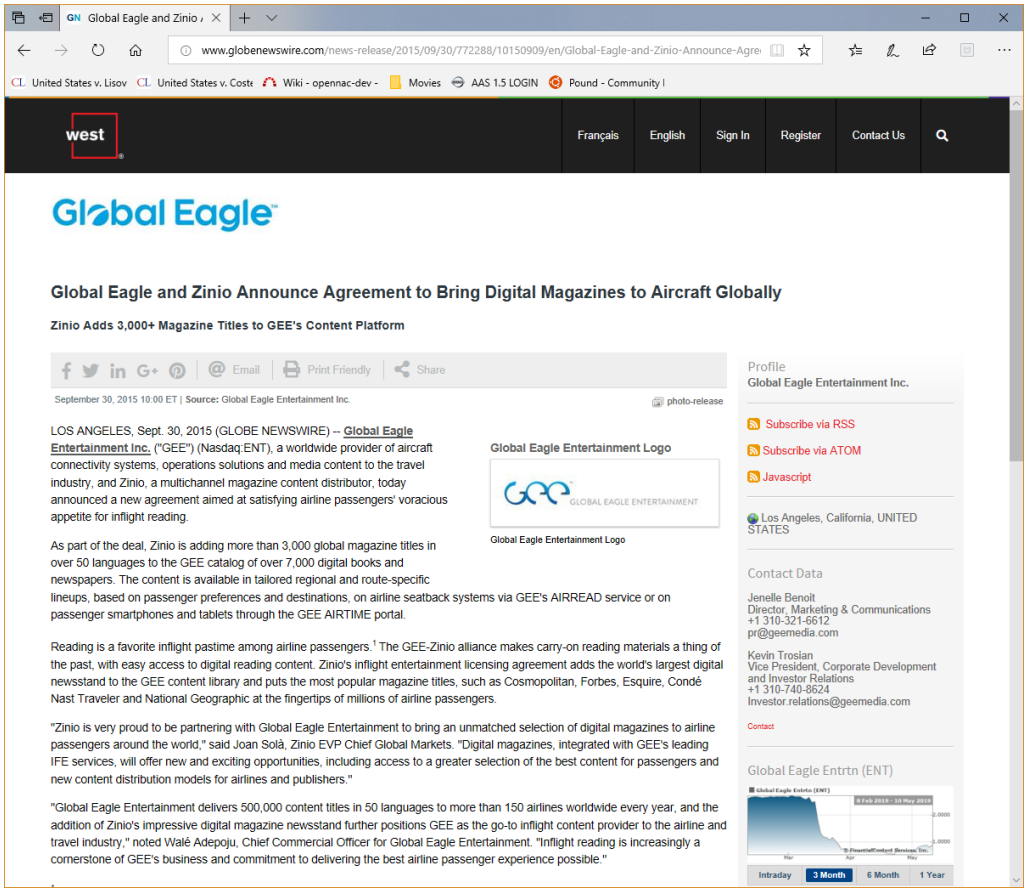


Figure 8 Obtenido de http://www.globenewswire.com/news-release/2015/09/30/772288/10150909/en/Global-Eagle-and-Zinio-Announce-Agreement-to-Bring-Digital-Magazines-to-Aircraft-Globally.html

4) Una vez que la información estuviera en sus servidores, era publicada al mercado negro en el internet para la venta.
5) El *broker*(s) compraba la información previamente adquirida del mercado negro en internet a Vadyn Iermolovych la cual utilizaría para realizar sus inversiones.
6) Luego se crean compañías fantasmas para lavar el dinero de las transacciones.
7) El *broker* realizaba las inversiones en el mercado de la bolsa de valores y se genera ganancias financieras debido a su ventaja competitiva.

SECCIÓN 4: INFORME DEL CASO

Resumen Ejecutivo

La oficina del fiscal del distrito de New Jersey contrató los servicios de Guard Active & Associates con el propósito de poder investigar, analizar y ayudar con el levantamiento de posible evidencia que pueda ayudar en el caso USA vs. Vadym Iermolovych. La responsabilidad de la empresa en la investigación está limitada al análisis y levantamiento posible evidencia y no incriminar o acusar a los involucrados.

Para la investigación nos enfocamos principalmente en el análisis de un dispositivo tipo USB de almacenamiento de datos obtenido del perpetrador Vadym Iermolovyc. Durante el proceso investigativo se identificaron múltiples documentos en formato PDF, JPEG, GIF, Word e imágenes de web sites. Entre los documentos se pudo identificar varios de los cuales contenían información relacionado a negociaciones y temas de activos en la bolsa de valores que no habían sido publicados aún. Lo cual sugiere que fueron obtenidos de las víctimas PRN.

Por la evidencia encontrada todo parece indicar que en efecto el Sr. Iermolovyc tuvo accesos no autorizado en las empresas PRN. Todo indica que los documentos encontrados en el dispositivo entregado para inspección de la incautación eran vendidos a terceros con el propósito de adquirir ganancias monetarias.

Dado concluida la investigación y revisado detalladamente los documentos encontrados y potencial evidencia encontrada apuntan a que en efecto los documentos pudieron haber sido adquiridos de PRN Newswired sin autorización y vendidos a terceros con el propósito de adquirir beneficio monetario. De la documentación inspeccionada se levantan datos que apuntan

a unos terceros (*brokers*) que realizaban la compra de los documentos para obtener beneficio competitivo en el mercado de valores.

Objetivo

El objetivo en la investigación está enfocado primordialmente en poder identificar o levantar potencial evidencia que ayude a esclarecer o fortalecer el caso USA vs Vadym Iermolovyc. Parte del proceso será el análisis cuidadoso de un dispositivo USB de almacenamiento de datos entregado a Guard Active & Associates por el fiscal del caso. El dispositivo contiene datos obtenidos de la máquina utilizada por el perpetrador para realzar los actos delictivos.

Alcance del trabajo

Guard Active & Associates utilizará la herramienta *OSForensic* con el propósito de levantar una copia de la imagen en el dispositivo de almacenamiento de datos USB. Luego procederá con el análisis y revisión de los hallazgos. La investigación estará comenzando el 3 de diciembre de 2016. De los hechos encontrados en la investigación se procederá con la presentación de un informe detallado.

Datos del caso

Número del caso: 16-CR-00235

Caso: USA vs Vadym Iermolovyc

Examinador: Guard Active & Associates

Cliente: *Assistant U.S. Attorney Sarah Devlin*

Descripción de los dispositivos utilizados

Los equipos y herramientas utilizados por Guard Active & Associates para realizar las investigaciones fueron:

- computadora portátil marca HP modelo EliteBook con 16 GB de memoria RAM y 500 GB de disco duro y un sistema operativo Windows 8.1.
- Para realizar el análisis del USB se utilizó la herramienta *OSForensic* para inspeccionar la imagen entregada por el fiscal.

Resumen de hallazgos

Durante el proceso de revisión y levantamiento de posible evidencia se logró identificar varios documentos en formato PDF, Word con datos relacionados a posibles inversiones o decisiones de negocio cuya información no estaba disponible aún para el público en general. En adición se pudo observar algunas páginas tipo HTML con datos adicionales para ser publicados. Entre los documentos encontramos uno titulado *Volvo Cars merge* el cual muestra la publicación de una posible unión entre la empresa Volvo Cars y Geely (empresa de Hong Kong). Otro de los documentos encontrados nombrado *All News Releases Distributed by PR Newswire* tenía contenido de empresas como *Kellogg Company* el cual anunciaría el retiro voluntario por su parte de los *Honey Smacks Cereal* debido a un potencial riesgo de salud. Una noticia que seguramente afectaría a la empresa. Estos y otros documentos encontrados en la imagen obtenida del ordenador personal del acusado son clara evidencia que lo posicionan directamente con las acusaciones en su contra.

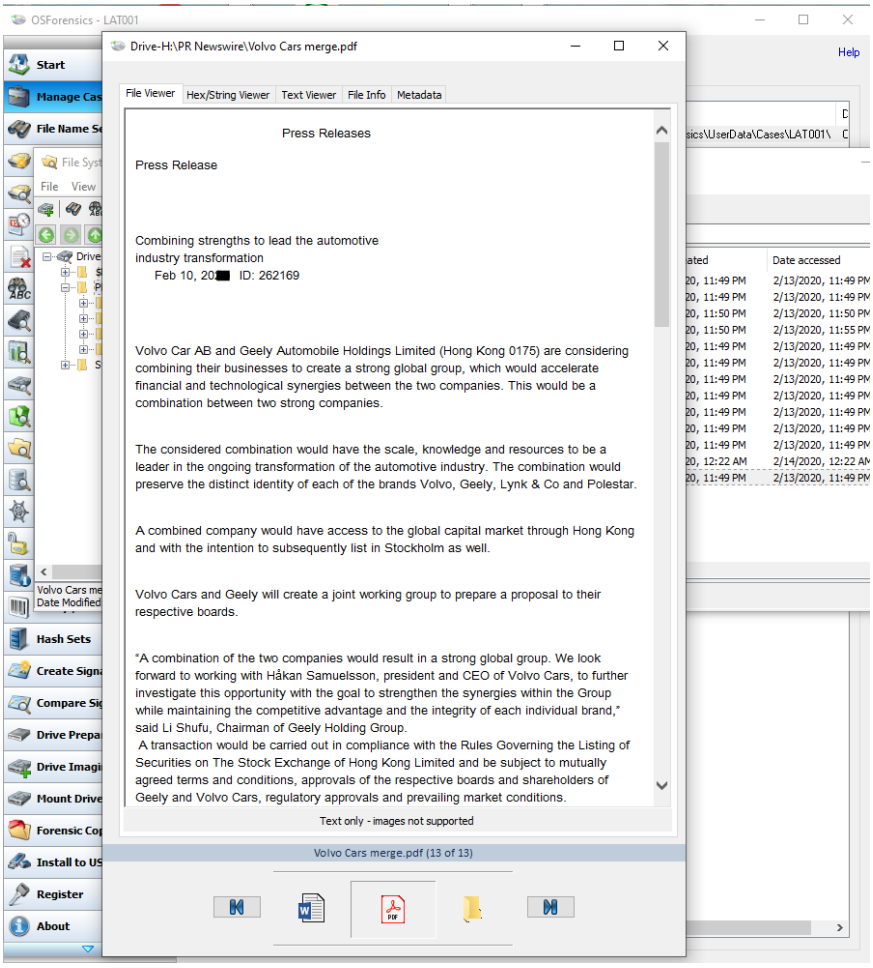


Figure 9 - Volvo Cars joint with Geely

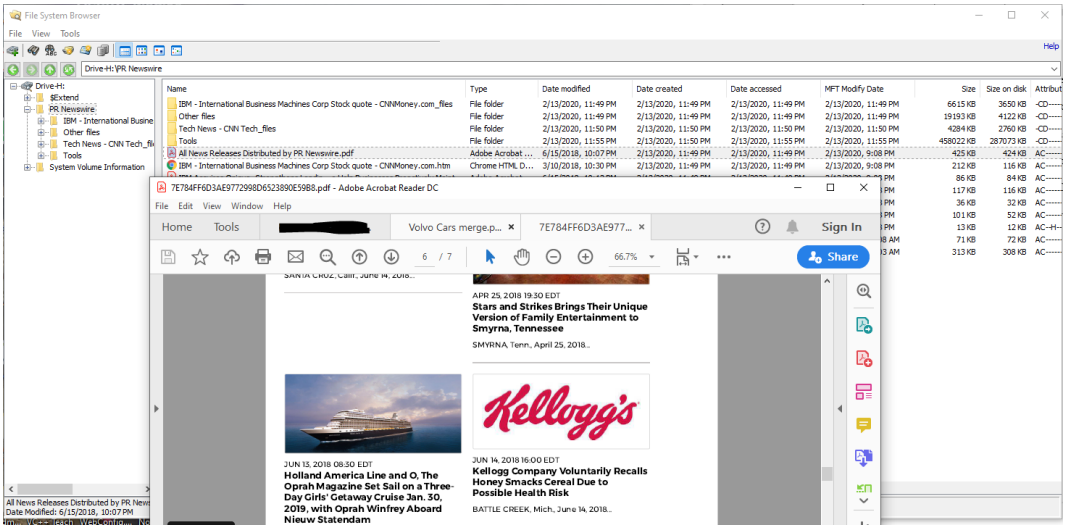


Figure 10 - Kellogg Company Voluntarily Recalls Honey Smacks Cereal

Cadena de custodia

Como parte de nuestro compromiso y responsabilidad se estableció un registro del manejo de la evidencia entregada por el fiscal a Guard Active & Associates. A continuación, desglose y detalle de la custodia de la evidencia.

Caso#:	16-CR-00235
Primer evento:	Entrega de copia de la evidencia.
Código de la evidencia:	2016-001-RM
Fecha y hora de comienzo: *Fecha y hora de terminado:*	1de diciembre de 2016 / 8:00 am 1 de diciembre de 2016 / 8:30 am
Comentarios:	La fiscalía hizo entrega de un dispositivo de almacenamiento de datos tipo USB. Guard Active & Associates tomo la evidencia identificada con el código 2016-001-RM y la misma fue guardada en bóveda.
Segundo evento:	Creación del caso de la investigación.
Caso#:	16-CR-00235
Código de la evidencia:	2016-001-RM
Fecha y hora de comienzo: *Fecha y hora de terminado:*	2 de diciembre de 2016 / 7:00 am 2 de diciembre de 2016 / 9:00 am
Comentarios:	Guard Active & Associates utilizando la herramienta de *OSForensic* crea el número de caso de la investigación.
Tercer evento:	Análisis y levantamiento de evidencia.
Caso#:	16-CR-00235
Código de la evidencia:	2016-001-RM
Fecha y hora de comienzo: *Fecha y hora de terminado:*	3 de diciembre de 2016 / 6:00 am 5 de diciembre de 2016 / 11:45 pm

Comentarios:	Se analizó el dispositivo con miras a poder encontrar evidencia adicional que pudiera incriminar al acusado.
Cuarto evento:	Entrega de evidencia
Caso#:	16-CR-00235
Código de la evidencia:	2016-001-RM
Fecha y hora de comienzo: *Fecha y hora de terminado:*	6 de diciembre de 2016 / 10:00 am 6 de diciembre de 2016 / 10:10 am
Comentarios:	Se hace entrega de la evidencia al fiscal.
Caso#:	16-CR-00235
Código de la evidencia:	2016-001-RM
Quinto evento:	Custodia de evidencia
Fecha y hora de comienzo: *Fecha y hora de terminado:*	6 de diciembre de 2016 /10:11 am 6 de diciembre de 2916 / 10:20 am
Comentarios:	El fiscal procede a llevar la evidencia a la bóveda para guardarla.

Procedimiento

En la siguiente sección estaremos detallando los pasos realizados en procedimiento de captura o análisis de evidencia. Se creó una copia de la imagen original para poder realizar el análisis y búsqueda de evidencia. Durante el proceso se utilizó la herramienta de *OSForensic*.

Creación del caso

Utilizando la herramienta de *OSForensic* se creó el caso ***2016-LRT-001***.

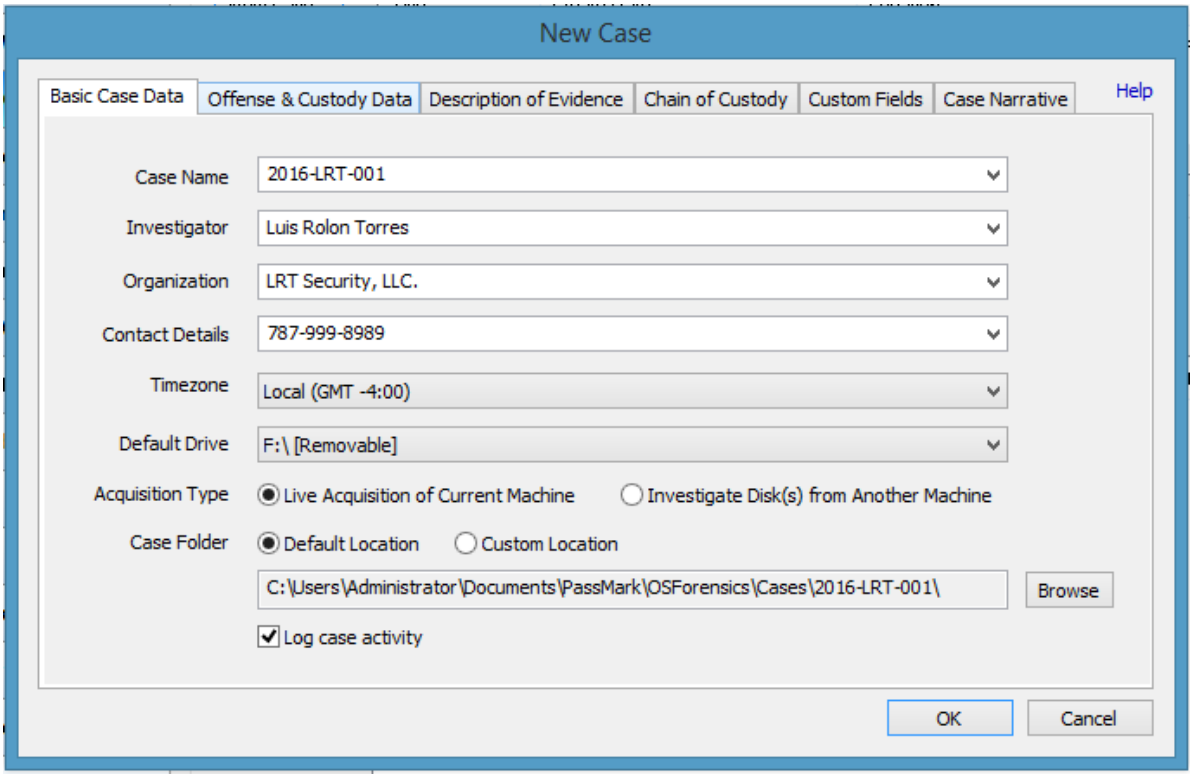


Figure 11 Creación del caso en OSForensic Tool.

Se procedió a crear el hash del file de la imagen como método de validar la integridad del mismo. (ver Figure 10)

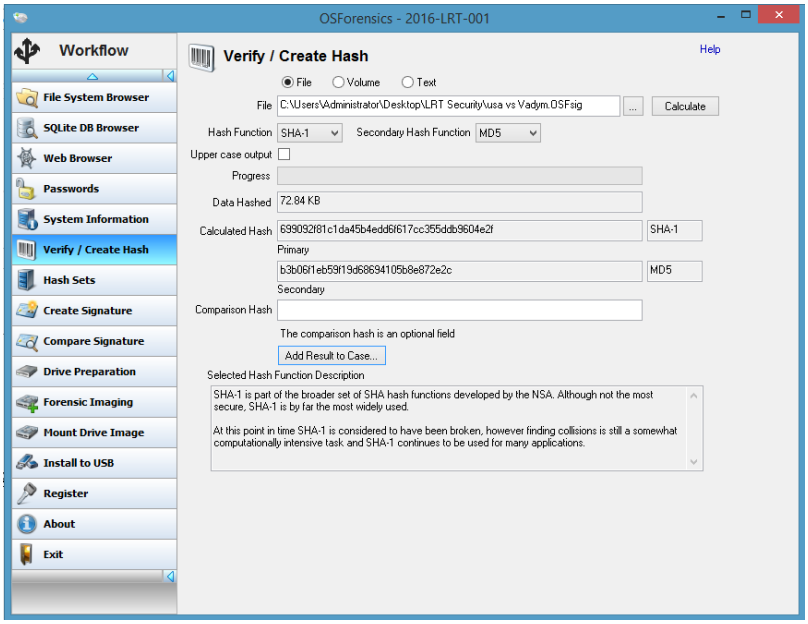


Figure 12 - Hash File

Luego de haber creado el hash para el archivo, se procedió a realizar la captura de la imagen al USB. (ver Figure 12)

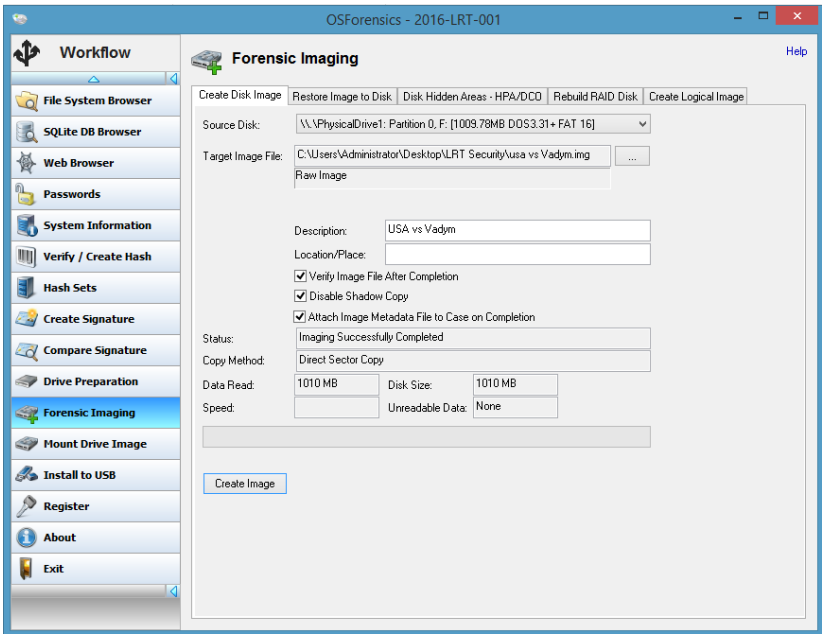


Figure 13 – Captura de la imagen del disco de la máquina del acusado.

Luego de crear la imagen y analizar su contenido encontramos algunos archivos los cuales tenían información sensible. De los archivos utilizados como evidencia se encuentra *Volvo Cars merge.pdf* y *All News Releases Distributed by PR Newswire.pdf* respectivamente.

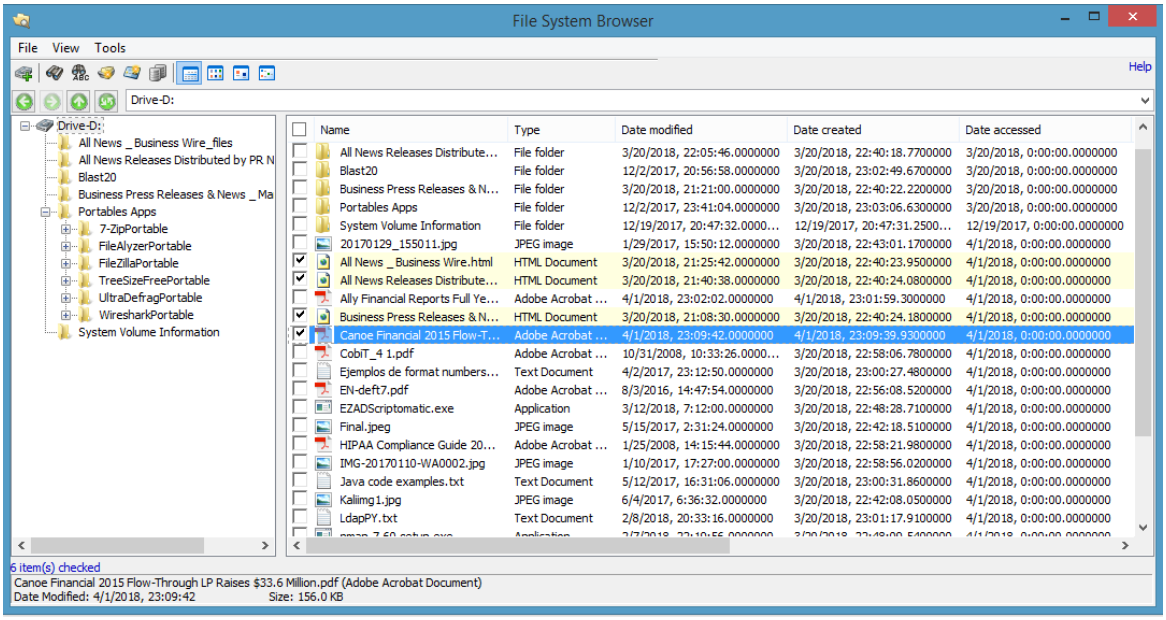


Figure 14 – exploración de evidencia

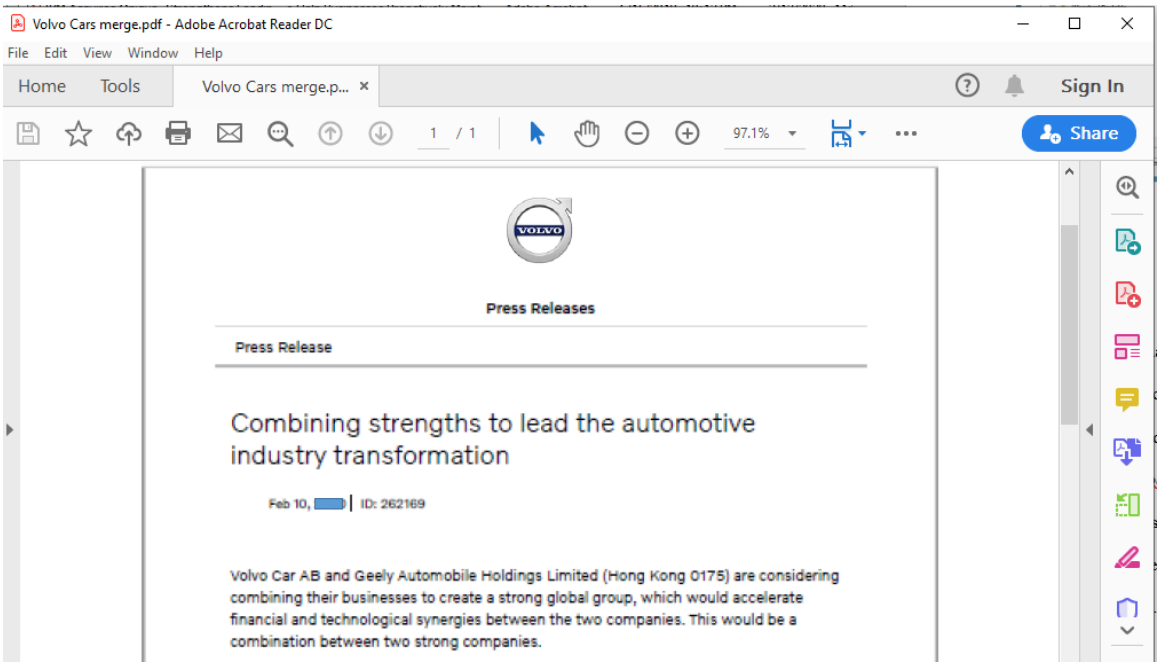


Figure 15 - Volvo Cars merge with Geely

Conclusión

Luego de haber evaluado la información suministrada por la oficina del fiscal del distrito de New Jersey todo parece indicar que el perpetrador (Vadym Ierlomovich) pudo haber obtenido acceso no autorizado a los servidores de las empresas víctimas (*Maketwired L.P. (marketwired), PR Newswire Association LLC (PRN) y Business wire*). La evidencia encontrada en la investigación muestra claramente que la información obtenida era de las empresas victimas vinculándolo así directamente con los cargos de los cuales se le acusa. Mostrando que el propósito principal del perpetrador era poder beneficiarse financieramente vendiendo la información adquirida.

SECCIÓN 5: DISCUSIÓN DEL CASO

De acuerdo con la información recopilada y evaluada en el caso de USA vs. Vadym Iermolovych (2016), todo apunta a que el acusado estuvo adquiriendo información de manera ilícita de las empresas Maketwired L.P. (marketwired), PR Newswire Association LLC (PRN) y Business wire. Según la información presentada el robo de datos se prolongó por varios años sin que se pudieran percatar de los hechos. Se alega que el Sr. Iermolovych a través de diferentes mecanismos de ataques como *brute force attack, SQL injection y Phishing* pudo obtener las credenciales necesarias para poder infiltrarse en los servidores y de ahí poder adquirir copia de los archivos. La información adquirida luego era vendida en el mercado negro a inversionistas.

Para poder tener suficiente evidencia que pudiera fortalecer el caso la fiscalía contrató los servicios de *Guard Active & Associates*. Estos investigadores realizaron un análisis de una imagen del disco duro de la máquina del acusado en el cual encontraron documentos y archivos que lo conectan directamente con lo presentado en su acusación. Parte de los documentos encontrados brindaban datos relacionados a productos que aún no eran públicos lo que daba la ventaja a los inversionistas que compraban los datos. Luego el Sr. Iermolovych envió una carta a la fiscalía haciendo alegación de culpabilidad por los hechos de los que se le acusaba. A este le fueron dado 3 cargos por fraude electrónico. Luego en el año 2017 el acusado tuvo una sentencia de 30 meses de cárcel.

SECCIÓN 6: AUDITORÍA Y PREVENCIÓN

Luego de haber analizado el caso de USA vs. VADYMIERMOLOVYCH se ha encontrado algunas de las posibles razones o fallas que permitieron el desarrollo del esquema de fraude contra las empresas Maketwired L.P. (marketwired), PR Newswire Association LLC (PRN) y Business wire. Algunos de los hallazgos identificados de acuerdo al contenido del caso y tomando en consideración los eventos o sucesos señalados por los acusados son las siguientes:

Hallazgo #1: Servidores sin actualizaciones correspondientes de "parchos" de seguridad del sistema operativo.

Criterio: Los servidores expuestos al internet deben estar debidamente parchados con las últimas actualizaciones de seguridad para minimizar o evitar la explotación de alguna vulnerabilidad.

Situación: Los servidores expuestos al internet fueron comprometidos.

Efecto: El no tener los servidores debidamente actualizados con los últimos parchos de seguridad permite que sea fácil el acceso a estos a través de ataques cibernéticos. En especial si la versión del sistema operativo es vieja, lo cual lo hace más vulnerable.

Causa: El personal a cargo de los servidores no revisa o instala los parchos de seguridad correspondientes a los servidores críticos de forma frecuente.

Recomendación: Es importante mantener un programa de *Patch managment* en la empresa el cual periódicamente se efectué la revisión e instalación de los parchos de seguridad recomendados para el sistema operativo en uso. De igual manera se debe revisar los parchos y vulnerabilidades de las aplicaciones de bases de datos utilizadas.

Hallazgo #2: La programación de la página web sin la evaluación adecuada de seguridad para el proceso de autenticación.

Criterio: las páginas que brindan servicio web deben seguir el *Software Development Life Cycle* en el cual se pueda mantener una programación libre de errores o vulnerabilidades a consecuencia de las revisiones y correcciones adecuadas antes de ponerla en producción.

Situación: los servidores de varias empresas fueron comprometidos con ataques de *sql injection* y *brute force attack* a través de la página web.

Efecto: el no utilizar un mecanismo de SDLC y no evaluar al detalle el código de la programación puede incurrir en crear zonas vulnerables que pudieran ser fáciles de explotar. Se pueden crear vulnerabilidades a través del error humano en el código basado en la logística del código o una falla en la versión utilizada creando el mismo efecto.

Causa: el personal a cargo de manejar el código y la logística de la programación no realizó las pruebas necesarias para poder identificar a tiempo potenciales vulnerabilidades en el código o la lógica del aplicativo.

Recomendación: es importante mantener un mecanismo de SDLC en el cual se evalué tanto el código de la aplicación como las vulnerabilidades de la versión de código utilizado. Existen herramientas específicas que pueden ayudar a minimizar grandemente estas vulnerabilidades. La herramienta *AppScan* de IBM es un ejemplo de una herramienta diseñada para evaluar el código y parte de la logística, aunque se recomienda una evaluación manual para garantizar su efectividad.

Hallazgo #3: Ausencia de protección adicional en el perímetro

Criterio: Toda empresa debe contar con la protección del perímetro adecuada de forma que se pueda proteger los equipos expuestos al internet utilizando *firewalls, IPS/IDS* y otros.

Situación: Los servidores expuestos fueron comprometidos utilizando *sql injection* y *brute force attacks*.

Efecto: El no contar con un equipo efectivo de protección en el perímetro puede comprometer todos los servidores que están expuestos al internet. De ser comprometidos se podría filtrar virus, *malware* y otros tipos de código malicioso con el propósito de acceder a información sensitiva de forma no autorizada.

Causa: El personal de tecnología no cuenta o no tiene configurado adecuadamente un sistema de IPS en el perímetro que pudiera servir de protección proactiva.

Recomendación: Al tener servidores expuestos en el perímetro es recomendable mantener un firewall con las configuraciones correspondientes que permitan únicamente el tráfico correspondiente según el tipo de servicio que brinda el servidor. En adición, se debe incluir un *Intrusion Protection System (IPS)* el cual pueda revisar el tráfico de entrada y de forma proactiva identificar potenciales ataques de *sql injection* y detenerlos antes de llegar al servidor.

Hallazgo #4: Falta de monitoreo o revisión efectiva del acceso a los servidores

Criterio: Es importante mantener un mecanismo de colectar y revisar periódicamente los eventos en los servidores críticos. Con el propósito de poder identificar potenciales filtraciones o ataques debe haber un proceso de *Event Managment*.

Situación: Al no contar con un mecanismo de *Event Mangement* el cual pudiera ser revisado con la frecuencia adecuada no se pudo identificar con tiempo la filtración de los ataques cibernéticos.

Efecto: Debido a que no todas las empresas afectadas pudieron detectar a tiempo el ataque o la filtración a sus servidores estos se comprometieron poniendo a la disposición del *hacker* toda la información que en ellos reside. A pesar de que PRN detecto meses después el *malware* no fue lo suficientemente efectivo ya que el daño había sido realizado.

Causa: El personal de IT no tiene configurado de forma efectiva la correlación de eventos para detectar poténciales ataques cibernéticos. Posiblemente no cuenta con un mecanismo de manejo de eventos adecuado.

Recomendación: Es importante mantener un sistema de *Event Managment* que tenga configurado las alertas correspondientes de forma que pueda crear una correlación de eventos e identificar rápido un potencial ataque o filtración a los equipos de la empresa.

SECCIÓN 7: CONCLUSIÓN

Luego de haber revisado y evaluado con detenimiento la evidencia provista por el Departamento de Justicia en el caso de USA vs Vadym Iermolovych se concluye que en efecto el acusado es culpable de los hechos de los cuales se le acusa. En este caso el propio conspirador se declaró culpable de haber obtenido acceso no autorizado a los servidores de las víctimas PRN y de haber vendido los documentos robados para su propio beneficio.

A través de las declaraciones del acusado se puedo concluir que estas empresas tuvieron muchas fallas internas que en su eventualidad llevaron a que fueran víctimas de Vadym Iermolovych. Entiendo que PRN tenía varias deficiencias operacionales que aportaron a que se explotaran sus vulnerabilidades. La falta de proceso de *Patch management* y monitoreo de eventos en los servidores y equipos de seguridad fueron factores claves que aportaron a potenciales ataques cibernéticos de fácil acceso.

En mi opinión, creo que toda empresa que trabaja con información sensible debe estar bien preparada con equipos debidamente actualizados, *firewalls* bien configurados, equipos o aplicaciones de manejo de eventos (*SIEM*) entre otros. Se debe tener en mente siempre el mantener un ambiente libre de vulnerabilidades enfocados en ser proactivos y no reactivos. Si PRN hubiese pensado en estos temas de protección posiblemente no hubieran sido víctimas de estos conspiradores quienes se lucraron por sobre 30 millones en todos esos años.

SECCIÓN 8: REFERENCIAS

18 U.S. Code § 1028A, Aggravated identity theft, Recuperado de https://www.law.cornell.edu/uscode/text/18/1028A

18 U.S. Code § 1028(a) (1) - Fraud and related activity in connection with identification documents, authentication features and information, Recuperado de https://www.law.cornell.edu/uscode/text/18/1028

18 U.S. Code § 1030 - Fraud and related activity in connection with computers, Recuperado de https://www.law.cornell.edu/uscode/text/18/1030

18 U.S. Code § 371 - Conspiracy to commit offense or to defraud United States, Recuperado de https://www.law.cornell.edu/uscode/text/18/371

18 U.S. Code § 1343 - Fraud by wire, radio, or television, Recuperado de https://www.law.cornell.edu/uscode/text/18/1343

18 U.S. Code § 1349 - Attempt and conspiracy, Recuperado de https://www.law.cornell.edu/uscode/text/18/1349

Acunetix (2019), What is a Reverse Shell, Recuperado de https://www.acunetix.com/blog/web-security-zone/what-is-reverse-shell/

Ámbito.com (2018), Empresas sufrieron nivel récord de fraude cibernético en 2017, Recuperado de http://www.ambito.com/912536-empresas-sufrieron-nivel-record-de-fraude-cibernetico-en-2017

Cisco.com (s.f.), What is Malware? , Recuperado de https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html#~types-of-malware

Cisco.com (2016), IP Addressing and Subnetting for new Users, Recuperado de https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html?dtid=osscdc000283

Condusef (s.f), Fraude Cibernéticos Tradicionales, Recuperado de https://www.condusef.gob.mx/?p=estadisticas

Court Listener (2015), United State v. Costea, Recuperado de https://www.courtlistener.com/docket/7309373/united-states-v-costea

Court Listener (2017), United State v. Lisov, Recuperado de https://www.courtlistener.com/docket/6291660/united-states-v-lisov/

Data Connectors (s.f.), 21 Terrifying Cyber Crime Statistics, Recuperado de https://www.dataconnectors.com/technews/21-terrifying-cyber-crime-statistics/

Gabaldón, L. (2006). Fraude electrónico y cultura corporativa. *Caderno CRH, 19* (47), 195-213.

Hernández, L. (2009). El delito informático. *Eguzkilore*, (23), 227-243.

Legal Information Institute (s.f.), Cornell Law School, PII (Personally Identifiable Information), Recuperado de https://www.law.cornell.edu/cfr/text/2/200.79

Legal Information Institute (s.f.), Cornell Law School, Computer and Internet Fraud, Recuperado de https://www.law.cornell.edu/wex/computer_and_internet_fraud

López Domínguez, I. (2015), Compraventa de activos financieros con pacto de retrocesión, Recuperado de http://www.enciclopediafinanciera.com/diccionario/compraventa-de-activos-financieros-con-pacto-de-retrocesion.html

Malwarebytes.com (s.f.), Suplantación de identidad (phising), Recuperado de https://es.malwarebytes.com/phishing/

Naciones Unidas. (2013). UNODC/CCPCJ/EG.4/2013/2, 1-18.

Nmap.org (s.f.), Nmap Introduction, Recuperado de https://nmap.org/

OpenWall (s.f.), John the Ripper password cracker, Recuperado de http://www.openwall.com/john/doc/

Oracle.com (s.f.), ATG Personalization Programming Guide, Recuperado de https://docs.oracle.com/cd/E26180_01/Platform.94/ATGPersProgGuide/html/s0506passwordhashing01.html

OWASP (s.f.), SQL Injection, Recuperado de https://owasp.org/www-community/attacks/SQL_Injection

PassMark Software (s.f.), OSForensic Professional, Recuperado de https://www.osforensics.com/downloads/OSF_help.pdf

Ramírez, E.E., & Aguilera, A. R. (2009). Los delitos informáticos: Tratamiento internacional. Contribuciones a las Ciencias Sociales. Recuperado de www.eumed.net/rev/cccss/04/rbar2.htm

Sánchez, G. (2012). Delitos en internet: Clases de fraude y estafas y las medidas para prevenirlo. *Boletín de Información*, 324, 67-88.

Sophos.com (s.f.), Brute force attack, Recuperado de https://www.sophos.com/es-es/threat-center/threat-analyses/threatsaurus/a-to-z-of-threats/b/brute-force-attack.aspx

TechTarget (s.f.), SQL (Structured Query Language), Recuperado de https://searchsqlserver.techtarget.com/definition/SQL

Tutorialspoint.com (s.f.), Ethical Hacking – Hackers Types, Recuperado de https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_hacker_types.htm

United States of America v. Vadym Iermolovych, United State District Court District of New Jersey, (2016), Recuperado de https://www.justice.gov/usao-nj/file/866486/download

United States Sentencing Commission, Guidelines manual (2015) (USSG), Recuperado de http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2015/GLMFull.pdf

W3Schools.com (s.f.), PHP Tutorial, Recuperado de https://www.w3schools.com/php/default.asp

Wikipedia.org (s.f.), Hacker, Recuperado de http://es.wikipedia.org/wiki/Hacker