El desconocimiento de las Pymes colombianas frente a las Amenazas Persistentes Avanzadas

Mora Franco, Christian Felipe
syncmax@gmail.com
Universidad Piloto de Colombia

Resumen — El presente artículo mostrará la apreciación subjetiva que se ha llevado a cabo durante el año 2014 sobre como las pequeñas y medianas empresas colombianas dan la suficiente importancia para aplicar la seguridad informática en sus infraestructuras, concretamente hablando sobre amenazas persistentes avanzadas conocidas por la sigla APT.

Se quiso evidenciar si las empresas conocen de esta definición y en caso de conocer el concepto, que están realizando al interior de las mismas para mitigar los procesos de hacking continuo que se está expandiendo a nivel mundial y que ha ocasionado múltiples ataques a grande escala afectando los pilares de la seguridad de la información como lo son la confidencialidad, disponibilidad e integridad.

Se debe tener en cuenta que para la realización del presente artículo, primero se realizó una exploración documental que permitió reunir la información suficiente que definiera el concepto de Amenazas Persistentes Avanzadas, características y su ciclo de vida, logrando determinar cómo los atacantes realizan una programación estratégica e inteligente de códigos complejos informáticos que les permita identificar el qué, cómo y cuándo atacar a los sistemas con gran nivel de precisión.

Adicionalmente la indagación se realizó a través de los procesos de consultoría e implementación/configuración de las diferentes soluciones informáticas destinadas para la protección de los sistemas, logrando entender la percepción que tienen las empresas sobre los ataques informáticos.

Con base en la experiencia profesional adquirida junto con los conocimientos adquiridos durante la especialización en Seguridad Informática, se procedió a realizar el presente artículo que se desarrolló como requisito para optar al título de Especialista en Seguridad Informática de la Universidad Piloto de Colombia.

Abstract — This article will show the subjective assessment that has been carried out during 2014 on how small and medium Colombian companies give enough importance to implement Computer Security into their infrastructure, specifically talking about advanced persistent threats better known with the acronym APT.

This wanted to see if companies know this definition and if they know the concept, what procedures performed in their organizations to avoid and mitigate the hacking processes that is expanding globally and has caused many attacks to large scale affecting the pillars of information security such as confidentiality, availability and integrity.

It should be noted that for the realization of this article, first documentary research was allowed and gather sufficient information to define the concept of Advanced Persistent Threats, characteristics and life cycle, achieving determine how attackers perform a strategic planning was performed and intelligent complex computer codes that allow them to identify what, how and when to attack the systems with high level of accuracy.

Additionally inquiry was conducted through consulting and implementation processes / configuration of different software solutions designed to protect systems, achieving understand the perception that companies have on attacks.

Based on professional experience with the knowledge acquired during specialization in Computer Security, proceeded to make this article which was developed as a requirement to obtain the title Computer Security Specialist from Universidad Piloto of Colombia.

Índice de Términos — Amenazas, infiltración, perdidas económicas, polimorfismo, sabotaje.

I. Introducción

La tarea ardua de proteger a las organizaciones contra las distintas modalidades de ataques está en constante ascenso debido a que los atacantes utilizan códigos inteligentes que ya no se basan en firmas de ataques sino que se adaptan a los sistemas y cambian su morfología haciéndose invisible frente a los sistemas de detección/prevención de intrusos, antivirus, anti spam y otros mecanismos de defensa.

De lo anterior surge el concepto de Amenazas Persistentes Avanzadas que está evolucionando a niveles donde pueden penetrar y afectar sistemas tan complejos que están ubicados en reactores nucleares, gobiernos, bancos, etc., afectando los

pilares de la seguridad de la información como lo es la Confidencialidad, Disponibilidad e Integridad.

En Colombia si bien hay numerosas empresas sobre todo imperando las pequeñas y medianas empresas y que están incursionando en las distintas industrias que mueve la economía nacional, no tienen en cuenta las problemáticas tecnológicas que pueden surgir en sus organizaciones sino hasta que ocurren eventos informáticos que no se estaban contemplando dentro de sus matrices de riesgos en caso de tener alguna o dentro de sus procesos productivos día tras día el cual se usa tecnología de punta y generando información que es uno de los activos más valiosos dentro de una empresa.

Con el peligro constante sobre la ciberguerra por parte de múltiples organizaciones que están dentro del mundo del hacking aplicando sofisticadas estrategias de filtración y extracción hacia sistemas informáticos, se quiere llegar a plantear lo siguiente: ¿Las pequeñas y medianas empresas consideradas como Pymes en Colombia están conscientes de la existencia de las Amenazas Persistentes Avanzadas que son conocidos con la sigla APT? Y si se tiene conocimiento del concepto ¿Qué están realizando las empresas para contrarrestar esas amenazas?

De acuerdo a los interrogantes y basado por la experiencia adquirida en el campo de la Seguridad Informática aplicada en clientes de distintas industrias, el presente artículo dará respuesta al planteamiento anterior partiendo del hecho de conocer un poco más sobre Amenazas Persistentes Avanzadas (APT).

II. DEFINICIÓN DE AMENAZAS PERSISTENTES AVANZADAS

De acuerdo con el Instituto Nacional de Normas y Tecnología de los Estados Unidos (NIST) define a las amenazas persistentes avanzadas (APT) de la siguiente manera: “La amenaza persistente avanzada es un enemigo con características superlativas tanto en habilidad como en recursos que le permiten a través del uso de múltiples vectores de ataque ya se físico o cibernético generar oportunidades para alcanzar sus objetivos, que por lo general logra establecerse dentro de os sistemas tecnológicos de información de las organizaciones con la finalidad de extraer o filtrar la información hacia el exterior de manera constante y/o quebrantar o tropezar elementos valiosos de una misión institucional, un programa o una organización, o establecerse en un lugar determinado que le permitirá posteriormente realizar las acciones preconcebidas. Además, la amenaza persistente avanzada realiza un seguimiento a sus objetivos de manera iterativa durante un tiempo prolongado y adaptándose a los mecanismos de defensa del objetivo, y con la determinación de mantener el nivel de interacción necesario para ejecutar sus procedimientos de ataque.”[1].

Adicionalmente al ver más de cerca las tres palabras que conforman la sigla APT se puede indicar con mayor claridad el concepto:

Amenaza: Debe haber una motivación por parte de un atacante para explotar vulnerabilidades y conseguir con éxito el ataque planeado.

Persistente: Las APT no se limitan a tener un tiempo corto para aprovechar temporalmente una oportunidad de ataque sino que estas se mantienen por largo tiempo dado que cambian morfológicamente su estructura de acuerdo con la oportunidad de ataque que vaya transcurriendo en los sistemas, empezando por las brechas pequeñas que abren el camino para alcanzar progresivamente la información significativa o critica de las empresas.

Avanzada: El atacante debe tener una experticia de larga trayectoria en técnicas de explotación de vulnerabilidades y conocimiento profundo de las diferentes bases de datos de vulnerabilidades existentes para poder formar códigos complejos de explotación de acuerdo a los escenarios que se vayan presentando en el objetivo. De esta manera el atacante puede incluso revelar las vulnerabilidades que no se hayan detectado anteriormente y poder ampliar el espectro de ataque si bien quisiera hacerlo.

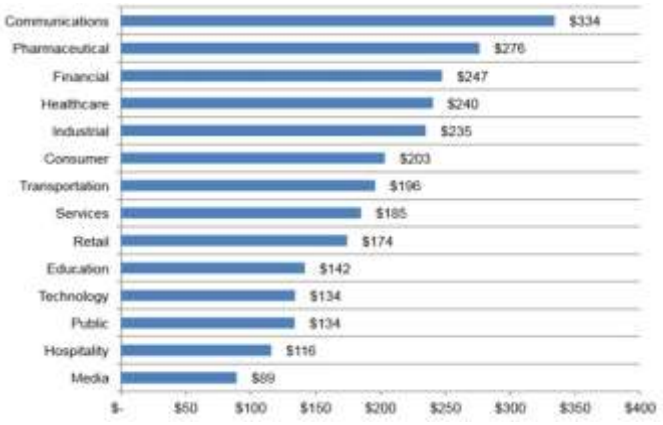
Teniendo en cuenta lo anterior los APT utilizan distintos vectores de ataque que pueden ser programados para atacar solo cuando encuentre la

oportunidad de atacar e infiltrase sin ser detectado gracias a su capacidad de actuar en bajo perfil, rompiendo las capas de seguridad que se haya implementado en las organizaciones.

Al realizar una retrospectiva en los últimos tiempos sobre grandes ataques se encuentra los casos de PlayStation de Sony el cual está prestigiosa compañía "sufrió una violación masiva en su red en línea de videojuegos que llevó al robo de nombres, direcciones y, posiblemente, datos de tarjetas de crédito pertenecientes a 77 millones de cuentas de usuario en lo que es uno de los robos más grande jamás vistos de seguridad en Internet." [2]

De acuerdo con estadísticas realizadas por Ponemon Institute haciendo una investigación sobre perdidas económicas por casos de violación de datos en las diferentes industrias en Estados Unidos se encuentra que en los últimos años se han perdido millones de dólares gracias al nivel alto de exposición de las diferentes compañías que no cuentan con una seguridad eficiente y robusta que minimicen la probabilidad de ocurrencia de afectación de los pilares de la seguridad de la información el cual en el siguiente grafico muestra el costo en millones por casos de violación de datos de acuerdo a la investigación realizada por Ponemon[3]:

Fig. 1: Pérdidas económicas por casos de violación a los sistemas informáticos



Fuente: http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf

Como la anterior grafica hay muchas estadísticas que revelan las cuantiosas pérdidas que las empresas a nivel mundial están expuestas a perder o que han perdido debido a la no pertinencia de contar con mecanismos de seguridad suficientes que mitiguen las amenazas que hay en el entorno, teniendo el pensamiento erróneo de manifestar que como son empresas que no son prestigiosas ni reconocidas a nivel mundial no son objetivos de atacantes cuando en realidad, hoy en día las empresas tanto pequeñas y medianas son los más interesados por los atacantes para realizas cualquier delito informático gracias a las vulnerabilidades que no han sido tratadas correctamente.

Luego de haber explicado brevemente sobre el concepto de APT y sus implicaciones dentro de las organizaciones a nivel mundial y el detrimento económico que puede generar por los ataques, a continuación se muestra como los atacantes hacen la planificación y estrategia del uso de los APT y como logran su cometido dentro de las organizaciones.

III. CARACTERÍSTICAS DE LAS AMENAZAS PERSISTENTES AVANZADAS

Las amenazas persistentes avanzadas son formadas gracias a una serie de características que les permiten tener la eficiencia, eficacia, adaptabilidad, sigilo y control sobre los sistemas informáticos que son objeto de amenaza para atacarlos en formas que son prácticamente imperceptibles logrando ser usados en grandes ataques masivos a escala global si así el atacante quisiera. De acuerdo con los autores Bodmer, Kilger, Carpenter, & Jones, definieron los criterios característicos que tienen los APT [4]:

Objetivos: Se plantea los objetivos previamente estudiados para realizar la explotación de las vulnerabilidades considerando los mismos como el adversario a tratar.

Oportunidad: Inspeccionar los momentos adecuados para poder realizar el ataque sin que sea interceptado por los mecanismos de defensa.

Recursos: Los niveles de experticia/conocimiento y las herramientas a utilizar para el ataque.

Tolerancia al Riesgo: Considera cada uno de los aspectos a tener en cuenta para que el ataque no sea sujeto de ser detectado.

Conocimientos y técnicas: Uso de las habilidades y herramientas más sofisticadas posibles para perpetuar el ataque con un gran nivel de éxito.
Acciones: Cada una de las tareas que están programadas específicamente para la amenaza o el conjunto de amenazas.

Puntos de origen del ataque: En búsqueda de los puntos donde se origina el evento.

Elementos involucrados en el ataque: Se precisa cuantos son los sistemas informáticos tanto internos como externos que participaron durante el ataque y cuantas personas estuvieron involucrados de acuerdo al peso de relevancia o importancia en los sistemas informáticos.

Fuentes de conocimiento: Hace distinción de toda la información recopilada en aquel sitio donde está la amenaza el cual se puede encontrar con información que revela más de lo que se necesita.

IV. CICLO DE VIDA DE LAS AMENAZAS PERSISTENTES AVANZADAS

De acuerdo con varios autores de distintas publicaciones, artículos o libros que hablan sobre Amenazas Persistentes Avanzadas, se ha evidenciado que típicamente tienen una serie de fases continuas que se utilizan para alcanzar los objetivos esperados:

Selección del objetivo a atacar: De acuerdo con las motivaciones que tiene el atacante, el mismo puede seleccionar uno o varios objetivos a alcanzar y que serán objeto de estudio y planificación de estrategia para determinar cuáles son los mejores escenarios para realizar el ataque.

Uso del Spear Phishing e Inteligencia Social: *Spear Phishing* es un método de Phishing que consiste en enviar correos provenientes en apariencia de entidades o personas conocidas pidiendo números de tarjetas de crédito, datos personales, cuentas bancarias, credenciales y un sin número de datos que pueden alimentar la información necesaria para que el atacante sepa cuál es el paso a seguir una vez conseguida los datos. Así mismo los atacantes pueden utilizar la Inteligencia Social indagando sobre comportamientos y/o actividades que realizan en la web donde las redes sociales y los blogs son materias primas importantes a la hora de conseguir información valiosa para el atacante.

Infiltración a través de sistemas comprometidos: Una vez identificados los sistemas computacionales que tienen vulnerabilidades para explotar, el atacante inyecta código que permitirá introducirse y colocar los tipos de malware que puede ejecutar de manera remota cuando la oportunidad se materialice para activar el software malicioso.

Persistencia: El atacante decide cuales son los momentos adecuados para poder ejecutar el código malicioso y proceder con el alcance del objetivo, el cual al terminar la ejecución puede lanzar comandos para dejar el malware en modo de espera para el siguiente ataque. Adicional a esto puede introducir más malware que permitirá apoyar y aumentar el ataque si es necesario para alcanzar el objetivo de una manera más precisa y audaz.

Obtención de la información: Con comandos pre configurados, el atacante puede hacer la extracción de información, realizar cambios drásticos en aplicaciones o bases de datos y/o estropear sistemas completos.

Borrado de huellas: el atacante realiza un barrido sobre las huellas dejadas en la ejecución de los códigos ejecutados para mantenerse en los sistemas y ser indetectable para el próximo ataque a lanzar.

Lo anterior no quiere decir que sean los pasos que utilizan los hackers en la actualidad sino que con base en el grado de experiencia y de acuerdo con las técnicas complejas que manejan

V. INVESTIGACIONES REALIZADAS POR FIRMAS DE CIBERSEGURIDAD

Adicionalmente firmas reconocidas en ciberseguridad como lo es Mandiant publicó un artículo donde muestra la investigación realizada desde 2004 a empresas de diferentes sectores que son objetivos de ataque, dando un enfoque a los procesos que tienen los grupos de hacker que están en China y que tienen definido un ciclo de vida de

los APT enumerando cada uno de los pasos que siguen los grupos conforme a los objetivos a alcanzar.
Un ejemplo de hackers de origen chino es el denominado *APT1* el cual fue objeto de estudio por parte de esta firma estadounidense arrojando estadísticas que preocupan sobre la seguridad de la red e infraestructuras: [5]

Fig.2 Ciclo de Vida de los APT del grupo APT1

Fuente: http://en.wikipedia.org/wiki/Advanced_persistent_threat

APT1 ha robado sistemáticamente cientos de terabytes de datos de al menos 141 organizaciones, y tiene demostrado la capacidad y la intención de robar a decenas de organizaciones simultáneamente.

De lo anterior se puede decir que los grupos de hacking sea en China o en diferentes partes del mundo ya tienen en su poder una infraestructura suficientemente robusta para poder lanzar ataques a escala global si así quisieran, robando cualquier tipo de información crítica de las diferentes empresas en cualquier sector o realizar todo tipo de sabotaje a aplicaciones e infraestructuras complejas logrando catástrofes a grande escala.

Incluso por medio del uso de las Amenazas Persistentes Avanzadas los grupos de hacking pueden incluso realizar todo tipo de extorsión en entidades gubernamentales del mundo realizando presión e influenciando a las masas para que se muevan en torno de estas organizaciones que buscan algún propósito en específico, dado que tienen motivaciones y argumentos para crear ataques masivos considerando cualquier entorno que sea vulnerable.

VI. EVALUACIÓN DE LAS PYMES EN COLOMBIA SOBRE APT

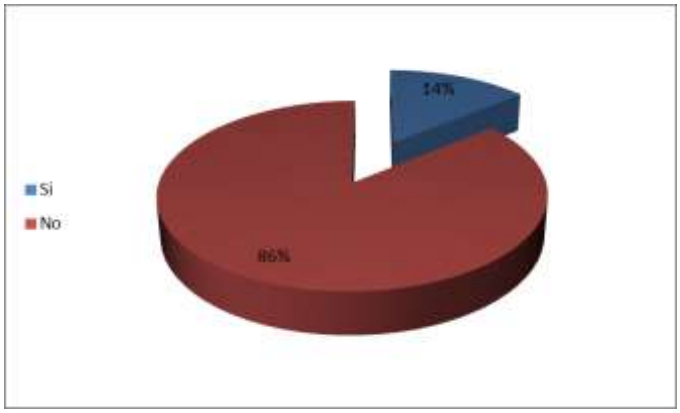
Pasando al entorno de Colombia y más concretamente en las Pymes con las que se ha logrado un trabajo en conjunto y que se han interesado en mayor o menor media sobre Seguridad Informática dentro sus instalaciones, se ha buscado establecer si las pequeñas y medianas empresas están familiarizadas con el concepto de APT y como este concepto ha tomado auge a nivel mundial de acuerdo con los hechos producidos en diferentes sectores industriales, sobre todo teniendo en cuenta que aquellos ataques fueron realizados por personas que tienen un amplio conocimiento en técnicas de penetración y extracción de información casi de manera imperceptible con la consecuencia de detrimento de imagen ante sus clientes, cuantiosas pérdidas económicas y más efectos devastadores.

Las compañías con las que se ha trabajado abarcan diferentes sectores industriales que van desde la farmacéutica, pasando por cadenas de restaurantes hasta llegar a comisionistas de bolsa y concesionarios de vehículos de alta gama.

Cabe decir que dependiendo de la actividad económica que realizan las compañías y el nivel de flujo de caja que mueve cada día, así mismo las empresas realizan los esfuerzos para adquirir soluciones informáticas que satisfaga la necesidad de estar protegidos frente las diferentes gamas de software malicioso, permitiendo que sus infraestructuras tengan la mayor protección posible haciendo valer el beneficio/costo ofrecidas por dichas soluciones.

El siguiente gráfico muestra cual es el porcentaje de los clientes que conocen o desconocen sobre que son las Amenazas Persistentes Avanzadas:

Fig. 3 Resultado Evaluación Subjetiva



Fuente: Propia del Autor

En todas las empresas ha llamado la atención que si bien conocen de sistemas perimetrales, antivirus, anti spam y demás mecanismos de defensa de diferentes fabricantes que existen en el mercado, la gran mayoría no conocen a ciencia cierta qué es y cómo actúan estas amenazas dentro de las organizaciones, a pesar de contar con personas que están dentro del campo de la seguridad informática.

El resultado de la evaluación sobre el conocimiento de APT revela que la mayoría de las Pymes demuestra que no están familiarizados con el concepto, dando una imagen preocupante sobre la seguridad que han implementado en sus infraestructuras tecnológicas, dando una impresión de una precaria consciencia sobre lo avanzado que están los ataques informáticos que realizan los grupos de hacking en el mundo, conformándose con solo tener ciertas herramientas de seguridad como lo son los antivirus que no ofrecen una protección completa frente a todo el espectro de malware, gusanos, troyanos y demás software malicioso.

También se ha identificado que las personas que tienen el poder de decisión sobre los proyectos tecnológicos no están apoyando de una manera significativa para realizar implementaciones de sistemas de seguridad que les permitirá estar protegidos ante cualquier amenaza externa, debido a que consideran que no benefician a nivel económico a las organizaciones por no contar con un retorno de inversión, el cual es un concepto errado porque si bien es cierto que es una inversión significativa en soluciones enfocadas a la seguridad informática en sus infraestructuras, las mismas mitigan el riesgo de alteración de la información generada en el día a día de las operaciones y que al no contar con estas soluciones pueden tener consecuencias letales que afectan la continuidad del negocio en esas empresas.

Con respecto a las Pymes que están familiarizadas con el concepto de APT, estas empresas han realizado esfuerzos en adquisición y capacitación sobre soluciones informáticas que les contribuya con la protección robusta en los diferentes elementos que componen la infraestructura tecnológica, considerando la importancia de estar al día en las innovaciones que los grandes fabricantes incentivan a sus clientes con la intención de maximizar la seguridad de la información.

Estas empresas que tienen a su disposición personas capacitadas y con experiencia en Seguridad Informática han motivado de maneras didácticas pero con el objetivo de tener en cuenta recomendaciones al momento de tratar información sensible de las operaciones realizadas durante el día, uso adecuado de los elementos informáticos, incluso reformado sus Sistemas de Gestión de Seguridad de la Información con cambios sustanciales en pro de la protección de las organizaciones junto con la implementación y puesta en marcha de soluciones informáticas que brindan protección en diferentes capas haciendo uso del concepto de Defensa en Profundidad.

Como medidas adicionales han contratado servicios de Ethical Hacking que les permita evaluar las posibles vulnerabilidades a los cuales están expuestas las organizaciones con el fin de validar si las medidas implementadas y configuradas de acuerdo con la necesidad de cada empresa está alineada con los objetivos planteados sobre las inversiones y esfuerzos realizados en seguridad y realizar las correcciones pertinentes.

Con lo anterior se puede evidenciar que a pesar que son muy pocas las empresas que están familiarizadas con las amenazas que son cada vez son más inteligentes y complejas no se quedan tener una posición reactiva frente a los posibles riesgos que puedan surgir sino que evalúan las mejores estrategias para enfrentar este flagelo informático

que está presente en cualquier tipo de industria a nivel mundial y que Colombia no es la excepción dado que las Pymes son los objetivos más pretendidos para realizar cualquier tipo de ataques.

VII. Conclusiones

En Colombia existen empresas que no le dan la importancia frente a las amenazas informáticas existentes que pueden aprovechar cualquier vulnerabilidad conocida y ser objetivos inminentes de personas o grupos especializados en realizar hacking y cometer delitos informáticos de toda índole capaz de alterar, manipular, sabotear y/o eliminar toda la información contenida en las grandes aplicaciones o bases de datos que las organizaciones utilizan en el diario vivir.

Se necesita grandes esfuerzos para contribuir con campañas de buen uso de las tecnologías de la información y la comunicación que permita abrir un espacio para la reflexión sobre la realidad a la que se está enfrentando dentro del contexto de los ataques informáticos, el cual al utilizar herramientas y técnicas avanzadas en cuanto a exploración, intrusión, adaptación y acciones deliberadas a través de códigos complejos creados con infinidad de motivaciones por parte de los atacantes y que cada día van evolucionando y perfeccionando su arsenal informático.

Es preciso decir que las empresas colombianas deben cambiar la mentalidad sobre la seguridad informática para que les sea una herramienta de apoyo que protegerá activos tan importantes como lo es la información y más teniendo en cuenta que las Amenazas Persistentes Avanzadas tienen la característica de cambiar la morfología de acuerdo con el ambiente que no dan descanso hasta encontrar la oportunidad de atacar de manera sigilosa pero al tiempo efectiva.

Si bien hay fabricantes que se especializan en soluciones que permiten proteger y cuidar de la infraestructura informática a las organizaciones, hay que tener en cuenta que el implementar y configurar todas las herramientas no es garantía de éxito contra los APT dado que se debe crear estrategias de mitigación de vulnerabilidades y aplicación de paradigmas como lo es la Defensa en Profundidad que por medio de capas permiten disipar con un alto porcentaje de efectividad ataques externos de cualquier índole.

Se considera que la seguridad informática es un proceso constante de evolución donde día tras día hay nuevas amenazas y vulnerabilidades que pueden ser explotadas de maneras impredecibles donde los esfuerzos de las organizaciones podrían no ser suficientes pero si le dan la verdadera importancia de aplicar esta disciplina pueden mitigar los riesgos y los impactos catastróficos cuando emplean Amenazas Persistentes Avanzadas.

REFERENCIAS

[1] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, (Publicación especial de NIST, Guía para realizar evaluaciones de riesgo) Disponible desde internet en http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf.

[2] REUTERS Sony PlayStation suffers massive data breach Disponible desde internet en http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

[3] PONEMON Institute. 2011 Cost of Data Breach Study: United States (2011 Estudio del costo de las violaciones de datos, Estados Unidos) Disponible desde internet en http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.

[4] BODMER, Kilger, Carpenter, & Jones (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. New York: McGraw-Hill Osborne Media. ISBN 0-07-177249-9, ISBN 978-0-07-177249-5

[5] MANDIANT. APT1: Exposing One of China's Cyber Espionage Units 2013 Disponible desde internet http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Christian Felipe Mora Franco, es Ingeniero de Sistemas egresado de la Fundación Universitaria Panamericana, Bogotá, Colombia; en la actualidad se desempeña Ingeniero de Soporte Especializado en una empresa integradora y consultora en Seguridad Informática y está optando al título de Especialista en Seguridad Informática en la Universidad Piloto de Colombia