SEPTIEMBRE 2015 / Nº 6

CIBER elcano

Desarrollado por:

INFORME MENSUAL DE CIBERSEGURIDAD

Copyright y derechos:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos-THIBER, the Cyber Security Think Tank

Todos los derechos de esta Obra están reservados a Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos y a THIBER, the Cyber Security Think Tank. Los titulares reconocen el derecho a utilizar la Obra en el ámbito de la propia actividad profesional con las siguientes condiciones:

a) Que se reconozca la propiedad de la Obra indicando expresamente los titulares del Copyright.
b) No se utilice con fines comerciales.
c) No se creen obras derivadas por alteración, trasformación y/o desarrollo de esta Obra.

Los titulares del Copyright no garantizan que la Obra esté ausente de errores. En los límites de lo posible se procederá a corregir en las ediciones sucesivas los errores señalados.

Eventuales denominaciones de productos y/o empresas y/o marcas y/o signos distintivos citados en la Obra son de propiedad exclusiva de los titulares correspondientes.

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank

Índice

1 Análisis de actualidad internacional....04

2 Opinión Ciberelcano....08

3 Entrevista a Román Ramírez....15

4 Informes y análisis sobre ciberseguridad publicados en agosto de 2015....21

5 Herramientas del analista....22

6 Análisis de los ciberataques del mes de agosto de 2015....24

7 Recomendaciones

7.1 Libros y películas....29

7.2 Webs recomendadas....31

7.3 Cuentas de Twitter....31

8 Eventos....32

1 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
Data brokers, el verdadero gran hermano

AUTORES: Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank.
Cybersecurity advisor, Eleven Paths (Telefónica).

Enrique Fojón Chamorro. Subdirector de THIBER, the cybersecurity think tank.

Qué son

Tras las filtraciones Edward Snowden en junio de 2013, se evidenciaron los grandes programas gubernamentales de captura y correlación de datos que permitían obtener, procesar y diseminar inteligencia basándose en el perfilado de sujetos y el establecimiento de relaciones.

Sin embargo, en la economía del siglo XXI, los datos son un negocio lucrativo, y el fenómeno del Big Data no ha hecho más que catalizar su valor comercial. En este contexto aparecen los *Data Brokers*, empresas privadas que recopilan información personal de consumidores y empresas, sustentando su modelo de ingresos en la reventa o compartición de dicha información sin la interacción directa de los usuarios.

Estas compañías recopilan datos personales como étnica, género, edad, ingresos anuales o afiliación política, usando dicha información para crear perfiles de consumidores, categorizándolos, por ejemplo, por perfil demográfico, político, ubicación del hogar, perfil financiero, salud o hábitos de consumo.

"Data Brokers, empresas privadas que recopilan de forma masiva información personal de consumidores y empresas"

El elenco potencial de compradores de estos perfiles es muy heterogéneo: desde departamentos de marketing de grandes compañías de productos de consumo que desean diseñar campañas orientadas a su público objetivo, a departamentos de I+D que requieren información sobre hábitos de consumo.

Pero ninguno de estos usos es, sin duda, tan preocupante como el que pueden realizar uno de sus grandes clientes: los gobiernos y sus agencias de información.

La actividad comercial de los *Data Brokers*, que comenzó a mediados de la década de 1970 como una evolución del telemarketing, ha visto una evolución exponencial con el auge y proliferación de las tecnologías de la información e Internet. Toda la información tiene valor, siempre existe un comprador que la pueda demandar.

Con el incremento del Internet de las cosas y un uso masivo de los dispositivos móviles, el volumen de información que genera la actividad diaria de cualquier usuario es enorme. Mediante su seguimiento, por ejemplo, a través de sensores ubicados en la calle o en los comercios,

se puede identificar la ruta que realizan los usuarios para ir a trabajar, los comercios que visitan y los tiempos de espera en el transporte público.

En 2012, la industria de los *Data Brokers* generó más de 150.000 millones de dólares en ingresos sólo en Estados Unidos, duplicando el presupuesto de inteligencia del gobierno norteamericano. En este sentido, no es extraño que la directora ejecutiva del Foro Mundial de la Privacidad declarara en el Senado estadounidense que "…la industria de los *Data Brokers*, tal y como es hoy día, no tiene limitaciones ni pudor. Venderá cualquier información, de cualquier persona, sin ninguna sensibilidad, a 7,9 centavos por nombre" o que la presidenta de la Comisión Federal del Comercio (FTC) estadounidense declarara el pasado año que "es una industria que opera fundamentalmente en la oscuridad".

Ante estos hechos, a instancias de la FTC, se elaboró un informe pormenorizado que analizaba la actividad de las nueve grandes compañías de data brokeraging norteamericanas, con operación en otros mercados internacionales: Acxiom, Corelogic, Datalogic, Ebureau, ID Analytics, Intelius, Peekyou, Rapleaf y Recorded Future.

El informe titulado *"Data brokers. A Call for Transparency and Accountability"* arroja luz sobre las prácticas corporativas de dichos actores en materia de la recolección, agregación y venta de los datos de usuarios a terceros. Entre sus principales conclusiones cabe destacar:

- El volumen de información recolectada por estas organizaciones es amplísimo. Sólo en el caso norteamericano, las nueve compañías analizadas aglutinaban 1.400 millones de transacciones comerciales, con más de 700.000 millones de elementos de datos, con un crecimiento mensual de 3.000 millones de entradas. En otras palabras, dichas compañías poseen información básicamente sobre cada ciudadano norteamericano.
- Los *Data Brokers* recolectan información masiva de multitud de fuentes – tanto públicas como privadas – sin el consentimiento explícito de los propios usuarios. Estos tipos de recolección no están regulados en muchos países, y en aquellos mercados con regulación específica relativa a la protección de datos personales (como puede ser el caso de la Unión Europea), esta recolección es abiertamente ilegítima.

- Estas compañías son capaces de combinar información tanto offline como online (a través de cookies por ejemplo) para inferir nueva información, en algunos casos, especialmente sensible.

Problema para la privacidad

La actividad de los *Data Brokers* no es ilegal en su naturaleza, pero tanto la legislación nacional como la europea hacen que estas empresas se hallen con mayores restricciones a la hora de operar en nuestro territorio. En la mayoría de los casos, éstos dependen de sitios web con aplicaciones de registro y cookies para encontrar a los consumidores online y enviarles anuncios por Internet basados en sus actividades fuera de la red. No obstante, en varios casos también utilizan otras fuentes – como el empleo de los sensores como puntos de acceso wifi – ubicados en la vía pública, comercios u hogares particulares – que pueden ser intrusivos con la privacidad de los usuarios.

"aquellas empresas que no actúen con transparencia y legalidad pueden ser objeto de sanciones económicas"

En este sentido, no es extraño que la Agencia Española de Protección de Datos declare repetidamente que aquellas empresas que no actúen con transparencia y legalidad pueden ser objeto de sanciones económicas. Sin embargo, aunque cada año ésta impone unos 20 millones de euros en sanciones, solamente puede operar contra aquellas empresas de titularidad española, que posean una filial en nuestro país o empleen para realizar las labores de data broking medios situados en territorio nacional.

A nivel más general, en Estados Unidos la FTC requirió al legislativo a que aprobara normativas que obligaran a los *Data Brokers* a ser más transparentes y que permitieran a los consumidores conocer la información que estas empresas poseen sobre ellos y sus hábitos de vida.

Pero existe otro problema menos conocido pero no por ello menos preocupante. Teniendo en cuenta que la mayoría de estas compañías almacena de manera indefinida los datos obtenidos ya que consideran necesario disponer de información evolutiva sobre los usuarios y así facilitar las labores de minería de datos histórico, los *Data Brokers* están siendo blanco de ciberataques dirigidos a robar su principal activo comercial: la información. El uso ilícito que pueda hacerse de tales volúmenes de información personal lo dejamos a la imaginación del lector, pero lo cierto es que sus efectos pueden ser estratégicos.

Data Brokers en el sector de la seguridad

Paralelamente, en los últimos años la demanda y uso de productos y tecnologías de seguridad ha aumentado significativamente. Con el crecimiento de este sector también ha aumentado drásticamente el volumen de datos de carácter personal que son recopilados, procesados, almacenados y compartidos entre distintas plataformas. Simultáneamente, la opinión pública se encuentra cada vez más sensibilizada con la necesidad de proteger dichos datos, con el objetivo de añadir transparencia al manejo de los mismos para así reducir las intrusiones en su privacidad.

La industria de los proveedores de servicios de ciberseguridad y seguridad convencional, debido al procesamiento y perfilado de datos que realizan, se convertido en una suerte de

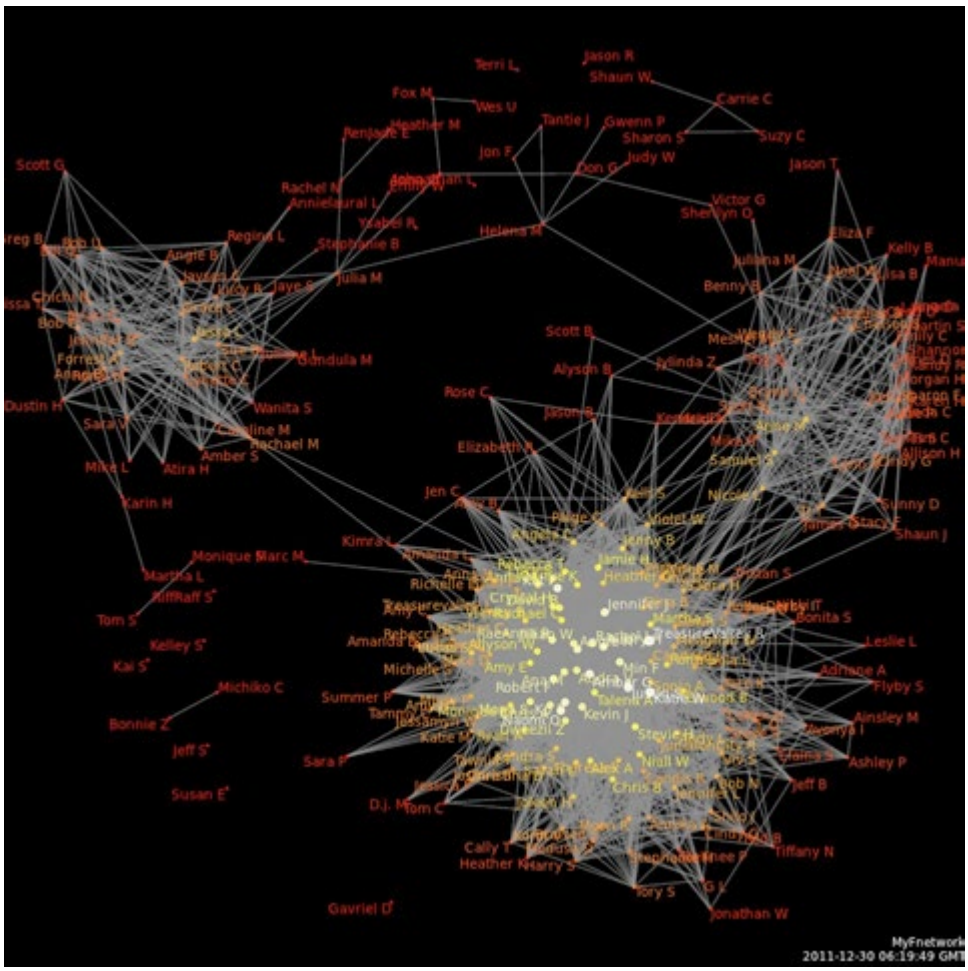
Data Brokers sectoriales, debiendo hacer frente a un desafío cada vez mayor relativo a la mejora de los mecanismos y procesos de protección de datos personales en sus tecnologías y servicios.

Ante este panorama, la Comisión Europea está actualmente trabajando, junto con los diversos agentes europeos de normalización, en el borrador de lo que será un futuro *estándar para la gestión de la privacidad en el diseño, desarrollo, producción y prestación de servicios de seguridad,* introduciendo el concepto de privacy by desing en la cadena de valor de este sector de la industria.

Conclusiones

A día de hoy nadie duda que la información personal pueda ser un negocio muy lucrativo. Con el surgimiento de Internet, la consolidación de la Era de la Información, las promesas del Big Data y el camino hacia el Internet de las Cosas, los datos se han convertido en algo vital de nuestra forma de vida. En este marco han aparecido los *Data Brokers*, empresas privadas que recopilan grandes volúmenes de información personal de consumidores o empresas y que revenden o comparten dicha información con terceros.

Las capacidades en materia de perfilado, las lagunas en materia normativa y los riesgos en materia de privacidad hacen de los *Data Brokers* un lucrativo negocio y un soporte a las agencias de inteligencia, que sirve como apoyo a muchas otras actividades empresariales, desde la toma de decisión en materia crediticia o aseguradora, a labores de marketing gracias al completo perfilado de nuestra personalidad y hábitos de vida o modos de consumo. Quizás por ello los *Data Brokers* son el gran hermano real del siglo XXI.



2 OPINIÓN CIBERELCANO

Análisis de la responsabilidad penal en la ciberseguridad de las personas jurídicas

AUTORES: Juan Antonio Frago Amada. Fiscalía Provincial de La Coruña.

Enrique Ávila Gómez. CoDirector del Centro Nacional de Excelencia en Ciberseguridad. Jefe de Servicio de T.I. Área de Operaciones. Dirección General de la Guardia Civil.

Preliminares

Como es bien sabido, la reforma del Código penal, operada por las Leyes Orgánicas 1 y 2/2015, respectivamente de reforma del Código y antiterrorista, publicadas ambas en el BOE de 31III2015, han venido, por un lado, a trasponer diversas directivas comunitarias, significadamente la 2013/40/UE, y por otro lado a adaptar la lucha contra el terrorismo a las nuevas metodologías de este tipo de delincuencia y adelantar las barreras de punibilidad a actos previos al acto central, el atentado, como puede ser la formación y el adoctrinamiento.

Desde el punto de vista de la ciberseguridad, entendemos que la mejor explicación de la reforma la ofrece la Exposición de Motivos de la LO 1/2015, apartado XIII, que hacia la mitad dice:

"La reforma lleva a cabo la transposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal.

Las modificaciones propuestas pretenden superar las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea.

De acuerdo con el planteamiento recogido en la Directiva, se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal: no es lo mismo el acceso al listado personal de contactos, que recabar datos relativos a la versión de software empleado o a la situación de los puertos de entrada a un sistema. Por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos.

Con el mismo planteamiento, y de acuerdo con las exigencias de la Directiva, se incluye la tipificación de la interceptación de transmisiones entre sistemas, cuando no se trata de transmisiones personales: la interceptación de comunicaciones personales ya estaba tipificada en el Código Penal ahora se trata de tipificar las transmisiones automáticas –no personales– entre equipos.

Se tipifica la facilitación o la producción de programas informáticos o equipos específicamente diseñados o adaptados para la comisión de estos delitos.

Se regulan separadamente, de un modo que permite ofrecer diferentes niveles de respuesta a la diferente gravedad de los hechos, los supuestos de daños informáticos y las interferencias en los sistemas de información.

Finalmente, en estos delitos se prevé la responsabilidad de las personas jurídicas ".

En suma, la ciberseguridad puede ser objeto de agresión tanto siendo el objetivo un bien de interés público (una infraestructura critica, por poner un ejemplo), como de interés privado (el tejido industrial español). Los ataques punibles se dividen, legalmente hablando, en delitos de intrusión (197 y ss Cp, denominados *"Del descubrimiento y revelación de secretos"*), infidelidad en la custodia de documentos y violación de secretos (413 y ss Cp), los daños informáticos o c racking informático (264 y ss Cp), y por remisión a los artículos ya señalados estas mismas conductas cuando se cometan con finalidades terroristas (573. 2 Cp), independientemente de que hablemos de una persona integrada en la organización terrorista o de que se trate de un "lobo solitario".

La comisión de delitos por personas jurídicas

La doctrina clásica del llamado Derecho continental venía preconizando que la comisión de delitos era cosa exclusiva de las personas físicas. Sin embargo, a principios del s. XXI se introdujo en España y la UE los principios anglosajones de responsabilidad de toda persona jurídica, de manera tímida al comienzo (art. 31. 2 Cp LO 15/2003), luego de manera más decidida (LO 5/2010, Ley 37/2011, LO 7/2012 y, finalmente, la LO 1/2015) para castigar los hechos cometidos por los administradores de las personas jurídicas, o bien por empleados que de manera directa o indirecta se aprovechasen de ellas, fuese o no posible individualizar el concreto autor del delito. Así, si un sujeto derrama productos contaminantes al río, en vez de seguir los cauces o protocolos de la empresa, la persona jurídica acabará respondiendo penalmente de ese ilícito, aunque no se pueda determinar quién haya sido el operario que produjo el vertido.

No es ocioso recordar que, tal y como cita el f. 2 de la Circular 1/2011 de la Fiscalía General del Estado, según el MaxPlanckInstitut für Ausländisches und Internationales Strafrecht, institución puntera del Derecho penal europeo, *"puso de relieve que ya entre los años 1974 y 1985, más del 80% de los delitos susceptibles de ser encuadrados en lo que se ha dado en llamar el Derecho penal económico, se cometían a través de empresas"*.

Ciñéndonos al ámbito de la ciberseguridad y dejando al margen otros sectores del Derecho penal, como el medioambiental, el económico, el del tráfico de drogas, etc., para los cuales casi todo lo que se dirá es casi asimilable, lo cierto es que nadie niega que son muy amplias las posibilidades que las nuevas tecnologías ofrecen a la delincuencia, desde muy diferentes aspectos. Por un lado, la inexistencia de fronteras en el ciberespacio ha provocado que la regulación existente, en la mayoría de los casos, no vaya mucho más allá de la mera cooperación policial y judicial en la persecución de estos delitos.

Por otra parte, y no menos importante por ello, la eclosión de nuevos actores que no se adscriben a ningún modelo clásico de la ciencia política, inducen la aparición de nuevos riesgos y amenazas que pueden ser difícilmente enfrentados utilizando las herramientas jurídicas clásicas de los Estados.

"aparece un rasgo fundamental en este tipo de delincuencia: la asimetría."

Por último y, según nuestra opinión, de crucial importancia, aparece un rasgo fundamental en este tipo de delincuencia: la asimetría. Los recursos necesarios para causar un grave daño son relativamente escasos y se encuentran más relacionados con la concienciación de los usuarios de las tecnologías de información (es decir, de todos los ciudadanos) y el entendimiento de los riesgos y amenazas a los que se enfrentan, que con los meros aspectos técnicos relacionados con la ciberseguridad.

Para una adecuada comprensión del problema analicemos un ejemplo completamente real: Los ordenadores de una conocida cadena hotelera se ven secuestrados por un pirata informático quien, desde las cuentas de correo de la antedicha cadena, ordena a su banco habitual que envíe 250.000 € a una tienda de La Coruña, la cual a su vez, previamente engañada, procede a remitir ese dinero a Singapur, perdiéndose así definitivamente su rastro.

Ni que decir tiene que atracar un banco es peligroso y que las consecuencias violentas de cualquier error pueden ser nefastas tanto para la víctima como para el delincuente: el atracador corre el riesgo de morir en el intento o pasar varios años en prisión por el contrario, el ciberdelincuente de nuestro ejemplo ha obtenido un botín no despreciable con absoluta impunidad y sin riesgo apreciable en la operativa seguida pues lo que ha hecho ha sido aprovecharse de desconocimientos y fallos en los procedimientos de la empresa involucrada.

Pero el ejemplo anterior no deja de ser una cuestión anecdótica al lado de muchos otros casos que cada vez tienen menos de fantasía y que se relacionan con la, cada vez, mayor dependencia de nuestra vida física de nuestra existencia virtual. A menudo pensamos en actividades racionales ejecutadas por personas. La eclosión de Internet de las Cosas dibuja un nuevo escenario en el que son algoritmos los que toman decisiones, en tiempo real, sobre actividades de nuestro mundo físico.

Si realizamos el esfuerzo intelectual de pensar con cuantos dispositivos inteligentes, es decir, con capacidad de cómputo, cada día, de forma consciente e inconsciente, interactuamos, más que probablemente no seremos capaces de nombrar más allá de los dispositivos PC, los mal

llamados teléfonos móviles (ya no son teléfonos sino terminales inteligentes de datos que, además, son capaces de realizar llamadas de voz) y, en el mejor de los casos, algún wearable tal como un reloj inteligente, que nos ofrece información tan interesante como nuestro ritmo cardiaco.

Posiblemente nos pasen desapercibidos dispositivos de tanto valor como el chip de nuestro eDNI o de nuestras tarjetas bancarias. O los sensores (cientos) de nuestro automóvil. O la tarjeta NFC de nuestro título de transporte público… Cada minuto interaccionamos con decenas de dispositivos inteligentes que tienen repercusión en la calidad de nuestras vidas.

Pensemos, por ejemplo, en nuestro nuevo contador digital de energía eléctrica. Seguramente no podríamos decir si nos lo han cambiado recientemente. Sin embargo, ¿qué pasaría si se infectasen decenas de miles de contadores dando como resultado lecturas erróneas de consumo eléctrico? Los resultados podrían ir desde la estafa masiva al ataque contra una infraestructura crítica al provocarse una parada de una central térmica o nuclear falseando los antedichos datos.

Desde una perspectiva menos apocalíptica se pueden dar hechos tales como el robo, de una empresa a otra de la competencia, toda la base de datos de clientes (caso ya acontecido), destruir esta misma base de datos, dejándola así inoperativa, o, aún peor, introducir información parcialmente errónea que provoque graves daños a su reputación entre sus clientes presentes y futuros.

Con posibles acciones adicionales cada vez más variadas y complejas de analizar desde el punto de vista jurídico, como el llamado delito de *astroturfing*, consistente en ir sembrando distintas informaciones por redes sociales, blogs, etc., de tal manera que vaya calando el mensaje de que tal o cual producto tiene una serie de beneficios o de perjuicios, con las consecuencias de ganancias o pérdidas que ello puede conllevar.

Si trasladamos este tipo de actividad, por ejemplo, al ámbito electoral, o a la elección de un consejo de administración, entre otros muchos supuestos, podremos extraer interesantes conclusiones relacionadas con los ámbitos de la Inteligencia y la ContraInteligencia.

A nadie se le escapa que cualquiera de estos delitos se puede acabar cometiendo por particulares y por personas jurídicas. Tampoco debe perderse de vista que el 90% de los delitos, salvo los de orden sexual y pocos más, se llevan a cabo con la finalidad de mejorar la propia posición económica o de perjudicar la ajena.

Sentadas estas premisas que la misma experiencia establece, acaba siendo de pura lógica que determinados delitos económicos, que se sirven de las nuevas tecnologías, se cometan para beneficiar a una persona jurídica o usando a otra como pantalla del ilícito.

"muy pocas empresas están adoptando realmente la figura del compliance officer o jefe de cumplimiento normativo."

La Directiva 2013/40/UE y la Ciberseguridad

La Unión Europea promulgó la Directiva 2013/40, relativa a los ataques contra sistemas de la información, con motivo de que muchos Estados miembros de la UE carecían de protección jurídica específica para dichos sistemas de la información.

Concretamente, los artículos 38 de esta Directiva prevén las concretas conductas que deben protegerse el art. 9 especifica las sanciones que han de imponerse a los particulares que las transgredan y, lo más importante a los efectos de este estudio, el art. 10 particularmente obliga a que los Estados miembros deben castigar los delitos cometidos tanto por los administradores de las personas jurídicas, como por empleados que hayan actuado en beneficio de estas, o si no se hubieran establecido los mecanismos necesarios para evitarlos.

Es decir, una persona jurídica incauta, cualquiera sea la forma que adopte (sociedad mercantil o civil, partido político, sindicato, etc.), puede acabar siendo condenada en el caso de que la fuerza investigadora concluya que algún tramo del llamado *iter criminis* ha pasado por la misma. Como podemos observar, una amenaza cierta contra la propia persona jurídica, con responsabilidad penal en caso de incumplimiento.

Sin embargo, muy pocas empresas están adoptando realmente la figura del compliance officer o jefe de cumplimiento normativo, que en el caso de personas jurídicas con un alto componente tecnológico o de protección de datos personales, puede suponerles la ruina.

Dice el nuevo art. 264 quater Cp:

"Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los tres artículos anteriores, se le impondrán las siguientes penas:

a) Multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años.

b) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos.

Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 delartículo 33. ".

La multa máxima de 5 años, calculada conforme al art. 50. 4 Cp, es de nueve millones de euros, además de que en el referido art. 33. 7 Cp se recogen la disolución de las personas jurídicas, suspensión de actividades hasta cinco años, clausura de locales, prohibición de actividades, inhabilitación para percibir beneficios o incentivos fiscales o de Seguridad Social y la intervención judicial, medidas que se pueden adoptar incluso durante la fase de instrucción (último apartado del art. 33. 7 Cp), no debiendo olvidarse que la anotación en el registro de contratistas públicos liquida sus posibilidades de llevar a cabo negocios con administraciones públicas.

Cuestiones para el porvenir

Sin embargo, el lento procedimiento judicial español, al que se le han de añadir las enormes dificultades de la persecución transfronteriza, hace que, a día de hoy, no sea muy práctico centrarse exclusivamente en la faceta represora del Derecho.

El Derecho penal de la persona jurídica, a través de lo que se viene conociendo como el *corporate compliance* , lleva a que el acento se deba poner en la faceta preventiva. Si en el ámbito sanitario se vacuna al individuo de las enfermedades de que podría contagiarse y tal vez contagiar a otros, o en cuanto a la seguridad ciudadana una patrulla policial consigue que en la mayoría de las ocasiones el delincuente desista de intentar el ilícito, en la ciberseguridad se hace necesario potenciar la prevención sobre la represión. Y a este respecto proponemos las siguientes líneas de actuación:

1) Formar convenientemente a personal de las FCSE en esta materia. Es un dato cierto que desde 2010 no se ha imputado ni por el BIT del Cuerpo Nacional de Policía ni por el GDT de la Guardia Civil a ninguna empresa por hechos con relevancia penal.

2) Formar a jueces y fiscales en esta especialidad. No es ocioso recordar la cita de Luis Jiménez de Asúa, el cual, en 1934 y prologando la obra de Rodríguez Sastre sobre el delito financiero, escribió:

"Hace sesenta años el español de presa, ansioso de despojar a otro de su fortuna o de sus ahorros, se echaba al monte, con clásico calañé y trabuco naranjero, escapando de sus perseguidores a lomos de la jaca andaluza.

Hoy crea sociedades, desfigura balances, simula desembolsos y suscripciones y, montado en la ignorancia de fiscales y magistrados, escapa sobre el cómodo asiento de su automóvil ".

Esta gran verdad de 1934 respecto a los delitos económicos, no demasiado desdibujada en 2015, viene a agravarse en el sentido de que el "delito informático" exige saber de Derecho, de derecho penal económico y de nuevas tecnologías. Y el problema se acentúa si no hay especialización judicial y si la policial o de la Fiscalía se caracteriza por la competencia en delitos informáticos, pero dejando más orillada la parte financiera del delito.

En resumen, según nuestra opinión, harían faltan equipos pluridisciplinares que aportasen lo que nos atrevemos a definir como capacidades en CiberInteligencia dada la complejidad de los asuntos a investigar, la asimetría de medios, las dificultades de persecución y, sobre todo, los tiempos involucrados a la hora de obtener cierta contundencia e inmediatez en la persecución de los antedichos delitos.

"a día de hoy, no es muy práctico centrarse exclusivamente en la faceta represora del Derecho."

3) Sensibilización del tejido empresarial y político del país sobre las verdaderas necesidades que la ciberseguridad exige. Legislar sin dotar de recursos para hacer cumplir lo legislado ya sabemos a qué conduce. Es mucho mejor generar un cuerpo normativo sencillo, rápidamente aplicable y con una suficiente dotación de recursos tanto para fiscalía y la judicatura como para las FCSE que perder el tiempo en legislar en detalle pero sin herramientas, tanto econó´micas como de competencias para hacer aplicar lo legislado.

4) Formación especializada en todas las capacidades relacionadas con lo que hemos denominado como CiberInteligencia, de tal manera que dispongamos de una visión omnicomprensiva de un problema complejo en el que la disponibilidad de recursos por parte de la persona jurídica puede acabar resultando el pretexto para la inactividad judicial o, peor aún , la incapacidad para determinar el dolo o la culpa de la misma frente a actividades delictivas realizadas haciendo uso de sus sistemas de información.

3 Entrevista a Román Ramírez.

Fundador de RootedCon. Responsable de Seguridad en Arquitecturas, Sistemas y Servicios. Ferrovial.

Todas las opiniones expresadas por Román en este artículo se hacen exclusivamente como representante de RootedCON.

1. Como director fundador y coordinador de RootedCON, uno de los congresos de seguridad técnica más reputados de Europa y de España, ha tenido la oportunidad de verificar el talento patrio en la materia a través de investigaciones y ponencias. ¿Están nuestros profesionales bien posicionados a nivel internacional?

La pregunta creo que tiene dos respuestas. La primera es una respuesta sobre el talento que tenemos en nuestro país, que es mucho y con unas capacidades excelentes. En general, se nos considera como excelentes profesionales en todos los apartados de la Seguridad de la Información y, en concreto en el mundo del hacking, tenemos de los hackers más reputados del planeta. Talento hay de sobra. PERO la segunda respuesta es que no, no estamos bien posicionados a nivel internacional, por las razones que voy a enumerar (obviamente, esta es mi visión sobre la situación que tenemos): primero, las bandas salariales en España son malas para las capas más técnicas (con diferencias enormes, de hasta sesenta mil euros al año en muchos casos), lo que hace que los mejores profesionales opten por marcharse fuera de nuestro país, o simplemente que pasen a empresas multinacionales extranjeras (donde se les paga un salario decente que reconoce sus altas capacidades). Esto deriva

en que el talento local, en vez de defenderlo, promocionarlo y mantenerlo (retenerlo, básicamente), lo formamos aquí para que lo aprovechen empresas extranjeras.

2. ¿Podría indicarnos cuál es su visión sobre los cambios de competencias de los profesionales de seguridad españoles? ¿Sería necesaria la definición de un marco de referencia de profesionales y competencias en materia de ciberseguridad?

Sinceramente creo que esas competencias existen ya. Son las mismas que se han venido desarrollando con la Seguridad clásica. Añadir el término “ciber” delante no cambia el espectro de conocimientos necesarios para ejercer una serie de funciones. Antes de plantearse marcos de referencia o competencias, creo que hay que conseguir transmitir correctamente un mensaje muy importante a las administraciones: un

perfil como el de un hacker no se consigue con los procesos tradicionales de formación, ni mediante un ciclo empresarial al uso. Mi opinión es que hay que equiparar la formación de un hacker con la de un francotirador, por ejemplo. El coste de preparar un francotirador de élite en los Navy Seal de EEUU ronda los 500.000 euros y 100.000 euros/año de mantenimiento. Esa es una muy buena referencia para entender qué tipo de capacidades y perfiles necesita este nuevo mundo en el que nos movemos. O comprendemos que los perfiles especializados cuestan dinero, o no avanzaremos (y seguiremos comprando soluciones a empresas extranjeras, con las evidentes consecuencias que puede tener esto en el contexto ciber).

"O comprendemos que los perfiles especializados cuestan dinero, o no avanzaremos"

3. Parece que hemos pasado de un tiempo a esta parte de una carestía de oferta formativa en seguridad de la información a un hype o sobresaturación de formación, tanto a nivel de certificaciones extra-académicas así como de postgrados en la materia. ¿Qué recomendaría a un profesional de seguridad que quiera iniciarse o mejorar sus aptitudes? ¿La oferta formativa española es adecuada?

La propia pregunta es autoconclusiva. Claramente hay moda ahora mismo alrededor de la seguridad de la información, los hackers, el ciber y el nuevo dominio de la ciberguerra. Pero eso no resta importancia y gravedad a la situación. Si nos ceñimos a los criminales estrictamente, ¿para qué me voy a meter en delitos de sangre que se persiguen con fuerza y tienen unas penas elevadas, cuando puedo dedicarme a infectar ordenadores sin demasiado riesgo y con poca alarma por parte de la sociedad? La industria del crimen tecnológico, en algunos casos, factura ya más que las tradicionales del narcotráfico y la rentabilidad asociada es más alta, puesto que el riesgo es menor. Además, creo que estamos asistiendo al nacimiento de esta nueva dinámica criminal; todo se agravará. Pero, ¿qué ocurre en el contexto de la guerra? La tecnología es amiga de la asimetría, luego podríamos estar hablando de países muy pequeños que, con pocos recursos, podrían lanzar ataques devastadores basados en vulnerabilidades en tecnología. Es normal que haya preocupación.

Por otro lado, la oferta formativa española es adecuada para preparar informáticos, abogados o profesionales de las fuerzas del estado, pero no lo es para preparar "francotiradores" (hackers). Vuelvo a mi comentario en la anterior pregunta: o interiorizamos la realidad a la que nos enfrentamos, o vamos a avanzar demasiado lento y con dificultades en capacitarnos adecuadamente.

4. Como consecuencia de la situación socio económica, hemos presenciado una importante fuga de talento nacional ¿Cómo frenaría la fuga de talento nacional hacia el extranjero? ¿Qué acciones debería tomar la empresa privada? ¿Y la Administración?

Sobre todo, pagar salarios dignos. Pretender que un especialista en ingeniería inversa o en crear exploits (herramientas de ataque) debe cobrar 30, 40 mil euros años es vivir fuera del mercado. Ahora mismo hay multitud de empresas que ofrecen desde 75 a 120 mil euros/año por este tipo de habilidades. Yo personalmente

he vivido situaciones kafkianas donde alguna persona del Mando de Ciberdefensa me ha venido a sugerir que deberían hacerlo por patriotismo. Yo me considero un patriota. Amo mi país, su cultura y su gente, pero tengo que llevar dinero a casa. La investigación en seguridad requiere de muchas horas, disciplina, mucho esfuerzo, estar en contacto con multitud de grupos de investigación y autoformación constante. Eso no se paga con 40.000 euros/año. Y, desde luego, menos todavía en empresas de body shopping y modelos similares. Pagando salarios dignos (subrayo, dignos), que estén en mercado y que demuestren respeto por las habilidades del especialista, estoy convencido de que mucha gente preferiría trabajar aquí que fuera.

"el proceso típico académico no forma hackers, forma profesionales informáticos"

Un problema grave es que, ese tipo de funciones, no aplican demasiado en la empresa privada generalista: no creo que haya demasiadas empresas IBEX35 que puedan requerir servicios de un "francotirador" (aunque sí de especialistas que te permitan defenderte de ellos). Y, adicionalmente, arrastramos demasiada inercia sobre lo que es y no es trabajar en seguridad, lo que hace que algunas empresas no se capaciten adecuadamente.

En la administración, en los profesionales de la defensa y las fuerzas policiales, sí veo un espacio más claro, pero hay que superar modelos absurdos y demasiado tradicionalistas para formar especialistas. Cosa que no comprendo, puesto que programas de formación para soldados o policías de élite existen, bastaría con incorporar contenidos relacionados con estos nuevos escenarios.

También hay que hacer comprender a muchos actores que el proceso típico académico no forma hackers, forma profesionales informáticos. Deben existir cambios en el entorno universitario.

5. Teniendo en cuenta su labor profesional en el sector privado, trabajando en una gran empresa cotizada ¿considera que los servicios y profesionales de seguridad españoles tienen una madurez adecuada para satisfacer las necesidades de una entidad como la suya?

En general, las empresas cuentan con los servicios que necesitan. Raro es el caso de una empresa bien gestionada que no se haya preparado para escenarios de riesgo de todo tipo. Es posible que sí podamos hablar de que haya que ampliar capacidades frente a amenazas más complejas como son las de gobiernos y grupos criminales especializados.

Pero el nivel en España es bastante bueno (basta con moverse un poco internacionalmente, para darse cuenta de que hay mucho tópico sobre lo bien o mal que pueden hacer las cosas las empresas anglosajonas).

6. Para aquellos profesionales especializados en la versión más técnica de la seguridad, ¿qué recomendación les haría si quieren llegar a ocupar puestos de responsabilidad en el mercado? ¿por cuenta propia o por cuenta ajena?

Esta es una pregunta especialmente complicada. ¿Qué son puestos de responsabilidad? Esta sí es una diferencia notable con otros países. En nuestro país existe un tópico malo sobre que la responsabilidad y las capacidades gerenciales

tienen que ver con venta (comercial), con jurídico o con financiero; en muchas empresas la carrera hacia puestos de responsabilidad suele pasar por salir de la parte técnica informática. En EEUU y otros países, existe carrera profesional en la vía tecnológica siendo el CISO, CSO, CHO (Chief Hacking Officer) o el CIO puestos en el *board* directivo del mismo nivel exactamente que los financieros, de recursos humanos o comercial.

Si tengo que responder en crudo, claramente recomendaría por cuenta propia, por experiencia propia puedo afirmar que es donde un perfil más especialista puede desarrollar su potencial. Aunque hay empresa españolas –sobre todo IBEX35—, donde sí se da la importancia que se debe al rol técnico.

Una recomendación **para todos los técnicos** (sean técnicos informáticos, financieros, de recursos humanos o técnicos jurídicos) es que aprendan las habilidades necesarias de gestión de personas, de contabilidad y finanzas, recursos humanos e informática.

7. Ante una potencial situación de indefensión ante ciberataques dirigidos y reiterados, ¿considera legítimo que las empresas españolas tengan cierta potestad para realizar una "respuesta activa" mediante mecanismos ofensivos para neutralizar el origen del ataque a expensas de las FCSE y de la Administración?

Personalmente creo que una parte importante de la defensa, es el ataque. Hablando en abstracto y a título de ensayo teórico, todas las organizaciones

deben capacitarse de igual manera en el **escudo** y en la **espada** (incluso en el puñal, la flecha, el explosivo o el veneno). Pongamos un ejemplo: una banda mafiosa ha lanzado una campaña de Cryptolocker que está infectando a cientos de empleados de una empresa. Un camino rápido para desactivar esa infección podría ser atacar sus centros de Mando (C&C) con algún tipo de capacidad ofensiva.

Pero nos enfrentamos a conflictos graves con el modelo democrático, puesto que el Contrato Social limita el ejercicio de la fuerza a los profesionales que los ciudadanos han autorizado para ejercerla, y nadie más. Para los delitos comunes son las FCSE, y en situaciones de conflicto bélico con otras naciones, el ejército y los agentes especializados en la guerra.

¿Cómo van empresas privadas a ejercer la "fuerza" aunque sea a título defensivo? ¿Deben existir empresas especializadas que puedan dedicarse a la "fuerza privada"? A mí personalmente las empresas de mercenarios me disgustan bastante; no hay más que analizar los comportamientos de organizaciones como Blackwater/Academi y otras para entender que no comparten el mismo concepto de honor y adhesión a una nación que un militar o un agente de la ley. Me espeluzna pensar en fuerzas privadas con capacidad policial o de guerra en mi país.

"los militares y las FCSE no tienen las capacidades ofensivas cibernéticas necesarias a fecha de hoy"

Pero claro, los militares y las FCSE no tienen las capacidades ofensivas cibernéticas necesarias a fecha de hoy, ¿qué hacemos cuando somos víctimas de un ataque cibernético y podríamos detenerlo con una respuesta rápida ofensiva?

El hecho es que, tras las revelaciones del caso Hacking Team, se ha hecho evidente que **distintos cuerpos de seguridad y agencias españolas**, han comprado herramientas ofensivas a esta empresa italiana. Quiero expresar con total claridad una opinión para llevar al lector a reflexionar: primero, es una vergüenza que se adquieran este tipo de soluciones a empresas extranjeras (existiendo un talento inmenso en nuestro país) y, segundo, cuando uno compra una herramienta de hacking a una empresa que puede estar sujeta a los intereses de otra nación, se arriesga a que esa herramienta esté "balizada" (para que las agencias de inteligencia de esa otra nación puedan rastrear su uso) o que ya haya sido vendida antes a vete tú a saber quién (cosa que se ha evidenciado con las filtraciones de Hacking Team). ¿No deberíamos poder hacer esto mismo con empresas locales especializadas y de mayor confianza?

Como comentario final, ¿y cómo podemos saber a ciencia cierta quién es nuestro atacante? Una cosa es que aparezcan sus direcciones de Internet como origen, y otra bien distinta que realmente sea ese el verdadero instigador del ataque. El proceso de **atribución** de un ataque es siempre **difícil y potencialmente dudoso.** Como el tan esgrimido origen del ataque a Sony que se ha utilizado para apoyar otros intereses; es altamente preocupante que EEUU afirme que ha sido Corea del Norte, en contra de la opinión de la comunidad de expertos en seguridad (existen diversas investigaciones independientes que apuntan a una exempleada enfadada colaborando con dos internos).

Es una situación *compleja* rodeada de otras complejidades en la **atribución** y la **legitimidad** de la respuesta ofensiva.

8. ¿Considera que existen vehículos de comunicación y colaboración adecuados entre los distintos órganos de la Administración (incluyendo FCSE) con los profesionales del sector? ¿De qué forma se podría optimizar y mejorar esta relación para conseguir una colaboración adecuada?

Claramente no, cuando hay descoordinación y objetivos conflictivos entre agencias policiales, servicios de inteligencia, ministerios, sector privado e intereses ciudadanos.

Un problema grave que veo es que, generalmente, las decisiones que se toman suelen venir empujadas por grupos de interés (lobbies) que tratan de mover a la administración hacia decisiones que les favorezcan (lobbies de la propiedad intelectual, lobbies de la seguridad privada, intereses comerciales como es el caso del TTIP,..) lo que, desde mi punto de vista, no responde a los intereses de los ciudadanos y, desde luego, tampoco a los de la defensa nacional. Las reformas de la Ley de Propiedad Intelectual, la Ley de Seguridad Ciudadana, la Ley de Seguridad Privada (y el tan cuestionado borrador de reglamento), LECrim… o, incluso, el tan infame Real Decreto de Autoconsumo, puede que no respondan directamente a intereses de los ciudadanos, sino a los de lobbies concretos. Los pongo como ejemplos que pueden llevar a decisiones equivocadas y peligrosas en la coordinación de las FCSE y la Administración.

"Es crítico conseguir que exista un punto único de coordinación cibernética que incorpore a todos los actores "

Es crítico conseguir que exista **un punto único de coordinación cibernética** que incorpore a todos los actores, que no esté sujeto a las presiones de lobbies sino que responda a los intereses del país y sus ciudadanos, que cuente con el talento necesario y la capacidad de ordenación, con capacidad sancionadora y, sobre todo, PRESUPUESTO.

En ese Punto Único deberían integrarse y aportar opiniones el Mando Conjunto, las FCSE, las agencias de inteligencia, CCN-CERT, INCIBE, representantes de los ministerios, universidades, organizaciones de profesionales, posiblemente ONG y organizaciones de derechos civiles y, por supuesto, **los hackers,** que son los que están más en contacto con lo que de verdad ocurre en las tripas de Internet y el Mundo Conectado.

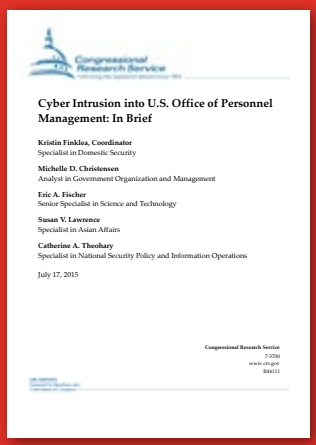
4 Informes y análisis sobre ciberseguridad publicados en junio de 2015

Cyber threat intelligence and the lessons from law enforcement (KPMG)

2015 Threat Report (Australian Cybersecurity Centre)

Hammertoos (Fireeye)

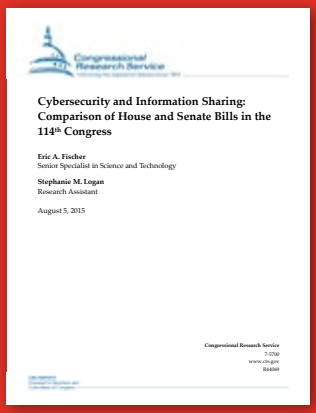
Cyber Intrusion into U.S Office of Personnel Management: In brief (U.S Congress)



Inventory of CERT activities in Europe (ENISA)

The Evolution of Cybersecurity Requirements for the U.S. Financial Industry (CSIS)

Cybersecurity and Information Sharing (U.S Congress)



Cyber-Enabled Economic Warfare: An evolving challenge (Hudson Insitute)

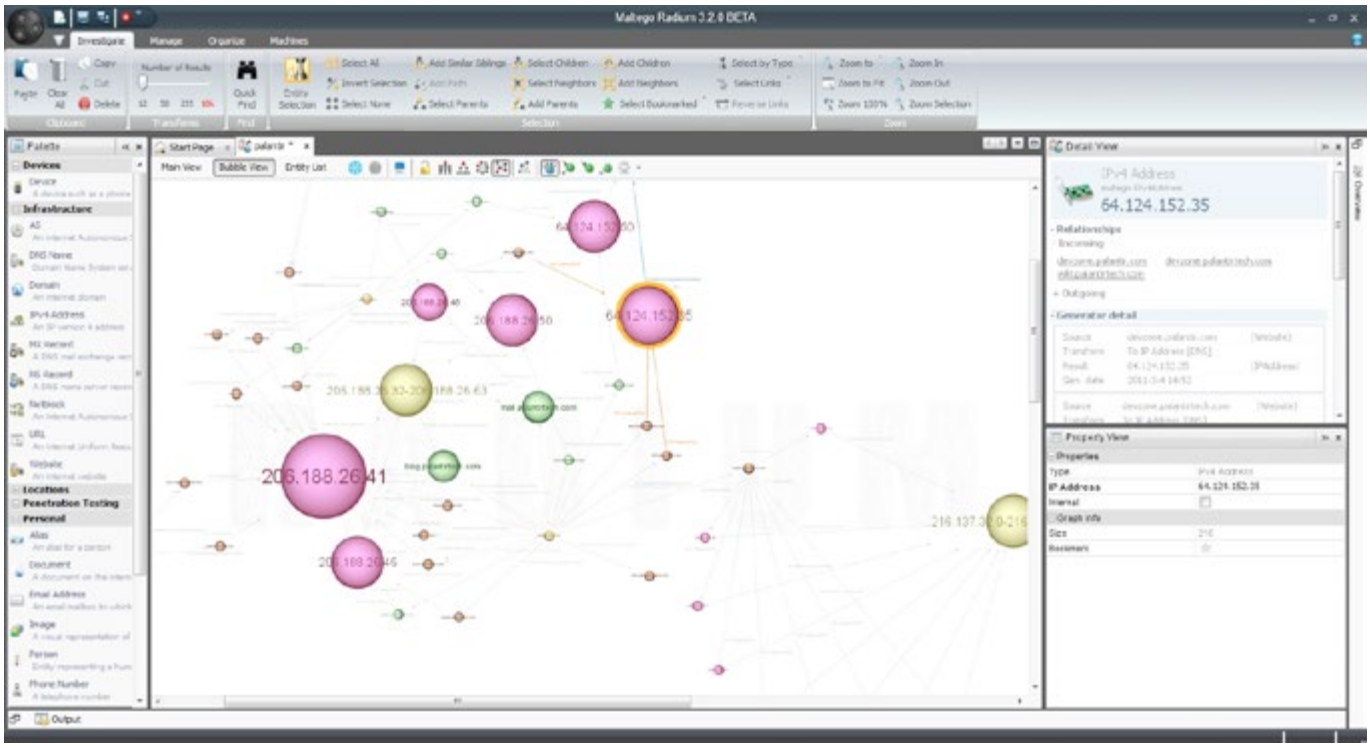
5 HERRAMIENTAS DEL ANALISTA: Maltego

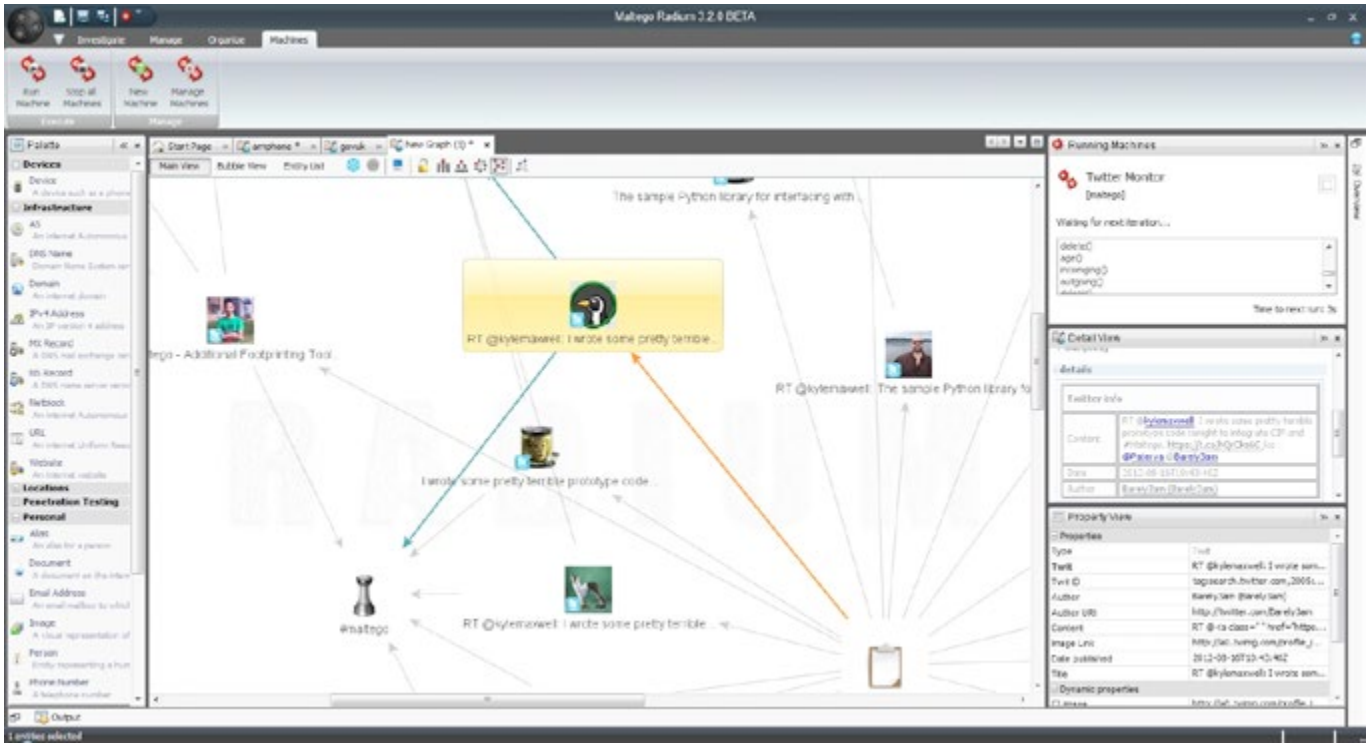
Maltego es un software propietario multiplataforma desarrollado en java y utilizado para soportar procesos de ciberinteligencia de fuentes abiertas y análisis forenses, desarrollado por Paterva, si bien *existe una versión community de libre acceso con algunas restricciones funcionales.* Maltego se centra en proporcionar una biblioteca de "transformadas" para el descubrimiento de los datos de fuentes abiertas, y la visualización de la información en un formato gráfico, adecuado para el análisis de relaciones y minería de datos.

Maltego permite crear entidades personalizadas, lo que permite representar cualquier tipo de información, además de los tipos de entidades básicas que son parte del software por defecto.

Las entidades Maltego define por defecto permite :

- Personas
- Grupos de personas (redes sociales)
- Compañías
- Organizaciones
- Webs
- Infraestructura de Internet:
  - Dominios
  - Nombres DNS
  - Netblocks
- Direcciones de red (IPs)
- Frases
- Afiliaciones
- Documentos y ficheros





Maltego se puede utilizar para la fase de recopilación de información de todos los trabajos relacionados con la seguridad de la información y el procesamiento de información digital, optimiza el proceso de razonamiento al demostrar visualmente vínculos entre objetos interconectados.

6 Análisis de los Ciberataques del mes de agosto de 2015

AUTOR: Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank.
Cybersecurity advisor, Eleven Paths (Telefónica).

El periodo vacacional ha presentado mucha actividad en el plano de la cibercriminalidad, protagonizado por uno de los ciberincidentes más mediatizados de los últimos meses, no por su criticidad, sino por el sensacionalismo asociado al mismo: el robo de datos de perfiles de usuarios de la web de contactos para adultos Ashley Madison.

CIBERCRIMEN

A principios de agosto, Avid Life Media, la compañía canadiense propietaria de Ashley Madison y webs como Cougarlife.com y EstablishedMen.com, reconoció haber sufrido un ataque en sus sistemas informáticos, si bien inicialmente no reveló la magnitud del mismo.

Ashley Madison es un conocido portal web de citas en línea que se dirige específicamente a las personas que buscan tener una Aventura. Tras el robo de datos, reclamado por un equipo denominado Impact Team, se han publicado los cerca de 37 millones de usuarios del portal

Los componentes de Impact Team publicaron los datos conteniendo millones de direcciones de correo electrónico. Entre los mismos, se han encontrado datos de funcionarios del gobierno de Estados Unidos, Reino Unido y otros países europeos, así como ejecutivos de alto nivel en empresas de Europa y América del Norte.

Tras la publicación del dump con los datos , según *diversos analistas citados en la CNN*, los servicios de inteligencia de China y Rusia están recopilando y analizando de los datos publicados, así como aquellos provenientes de la filtración de datos de la *Oficina de Administración de Personal (OPM).*, ya que entre ambos suman alrededor de 58 millones de perfiles de usuarios. Al cotejar y cruzar estos datos entre si, se puede comenzar a realizar un perfil de un usuario real con un nivel de detalle relevante y con información altamente sensible.

A comienzos de agosto, un equipo de *hackers ha atacado Carphone Warehouse* mediante un ataque de denegación de servicio distribuido (DDoS) como herramienta deceptiva, mientras robaban los datos personales y bancarios de 2,4 millones de personas, perpetrando uno de los mayores robos de datos de la historia de Reino Unido.

Junio y julio han establecido nuevos récords de ataques de publicidad maliciosa, denominados Malvertising. A principio de mes, *la red de publicidad de Yahoo (con más de 6.900 millones de visitas al mes), fue empleada para distribuir este tipo de malware.*

Tan pronto como se detectó la actividad maliciosa, se notificó a Yahoo!, tomándose medidas inmediatas para detener el problema. La campaña dejó de estar activa a las pocas horas.

Este mes se destapó una banda formada por un grupo de informáticos veinteañeros y veteranos traders, que mediante ciberataques obtenían los resultados de empresas cotizadas antes de que fueran conocidos por el gran público e invertían a través de derivados financieros para aumentar su poder de inversión. La SEC, el supervisor bursátil de EEUU, los acaba de destapar y describe su operativa en el *sumario* de acusación de la Fiscalía de Nueva Jersey.

Durante cuatro años, el grupo que operaba desde Odessa, Kiev (Ucrania), Moscú (Rusia), Glenn Mills y Alpharetta, dos pequeñas ciudades de Pensilvania y Georgia en EEUU; pudo obtener hasta 100.000 documentos financieros de PRNewswire Association LLC, Marketwired y Business Wire, una empresa propiedad de Warren Buffett.antes antes de que se publicasen en la SEC.

Una vez obtenidos los datos y cotejados con las previsiones de los analistas para cada empresa invertían al alza (con opciones call) o a la baja (opciones put) aprovechando los bruscos movimientos de las acciones cada vez que actualizan al público la evolución de su negocio.

CIBERESPIONAJE

Sobre el 25 de julio, funcionarios estadounidenses comunicaron a la NBC que Rusia puso en marcha un *"ciberataque sofisticado"* contra el sistema de correo electrónico no clasificado del Estado Mayor Conjunto del Pentágono, que fue sido cerrado y puesto offline durante casi dos semanas. Según los funcionarios, la "intrusión cibernética sofisticada" afectó a unos 4.000 usuarios entre personal militar y civil que trabajan para los jefes del Estado Mayor Conjunto.

Por otra parte, Sabre Corp., que procesa las reservas para cientos de aerolíneas y miles de hoteles, confirmó a mediados de agosto que sus *sistemas fueron atacados.* La empresa fue probablemente hackeada como parte de la misma ola de ataques que se dirigieron contra la aseguradora WellPoint y la oficina de personal del gobierno de Estados Unidos. Todos los casos fueron presuntamente ejecutados por el mismo grupo chino que ataco también Himno Inc.

Como ya pasó hace algunos meses, *a finales de agosto GitHub volvió a sufrir un ataque de denegación de servicio distribuido* siendo perpetrada por actores desconocidos.

Este es el segundo DDOS significativa GitHub ha sufrido en 2015 después de un incidente de marzo que vio el sitio atacado por entidades que al parecer quedaban ocultar tras el sistema chino conocido como la Gran Muralla.

El brazo canadiense de Anonymous, mandó un mensaje al Daily Show a través de un defacemente de la página web corporativa oficial de Donald Trump.

"Le escribimos hoy a través de la página web del Sr. Trump, ya que, al parecer, es la única manera de conseguir que nos presten atención", reza una versión archivada de la página Trump.com titulado "Tu Momento de Zen, el Sr. Stewart. "

Firmado por TelecomixCanada, la carta agradece a Stewart, por sus "muchos años felices de periodismo de calidad y entretenimiento" en The Daily Show.

www.trump.com/_common/2007/HTML_Editor/document.html

Your Moment of Zen, Mr Stewart

We are writing you today via Mr Trump's website because, seeming, the only way to get anyone to pay attention any more is to grease a Presidential candidate's website. We agree it is a regrettable state of affairs, we blame big Quinoa mostly.

.. but, we digress..

Mr Stewart, we at @TelecomixCanada would like to take this opportunity to thank you for the many happy years of quality journalism and entertainment you and your team have undertaken at Comedy Central. While even we, having wired live fire ustreams out of Gaza under Mossad's gaze, are unable to get Comedy Central's website video to work - undaunted we remain your loyal and grateful fans.

Understanding your technical interests remain unexplored you will probably be told of this by one of your most excellent producers. Know, Sir, that your steadfast dedication to the irony and power of Truth has inspired a generation which we ourselves now serve. That our collective thanks appears here will, we hope, amuse you as much as it will them.

We note, with some annoyance, that your natural opponents are beginning to talk smack about you (and presumably your mother).. Labouring, perhaps, under the misapprehension that it is once again business as usual while you enjoy your days tossing ball with the scion and evenings pursuing Mrs Stewart round the sofa with ice tongs.

Anonymous
@YourAnonNews
Follow

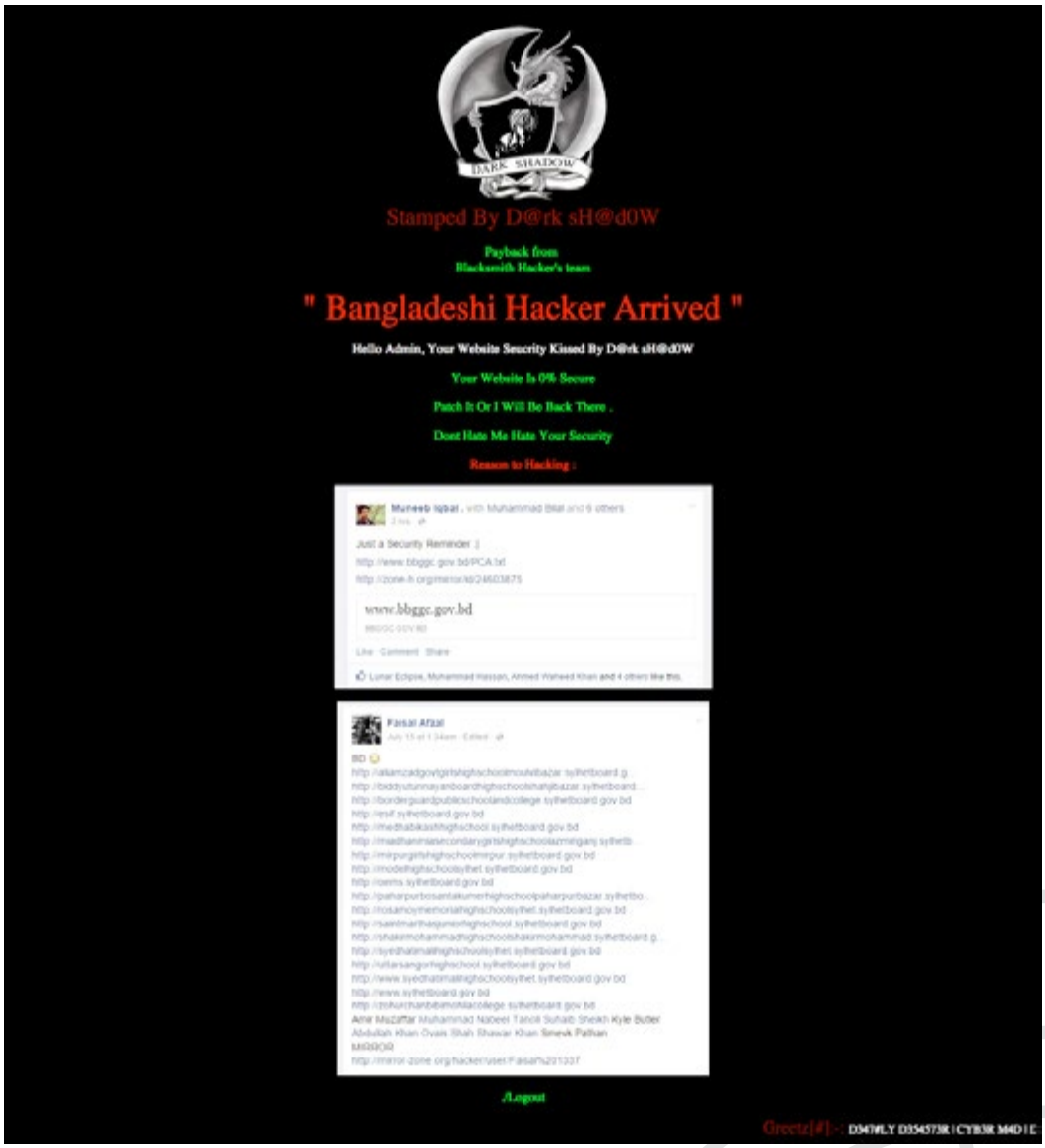
.@TelecomixCanada with an important message for Jon Stewart: trump.com/_common/2007/H… #MomentOfZen @TheDailyShow

2:01 PM - 3 Aug 2015

132 100

A finales de Julio, *el sitio web del presidente paquistaní Mamnoon Hussain fue objeto de un ataque de defacement* por piratas informáticos de Bangladesh - otros 72 sitios web del gobierno de Pakistán fueron también atacados.

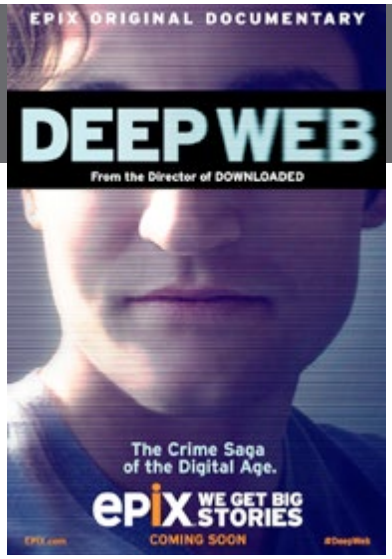
Parece existir un conflict cibernético continuo entre hackers de Bangladesh y Pakistán, donde un buen número de sitios web del gobierno están bajo ataque.



https://www.hackread.com/pakistani-president-website-hacked/

7 Recomendaciones

7.1 Libros y películas



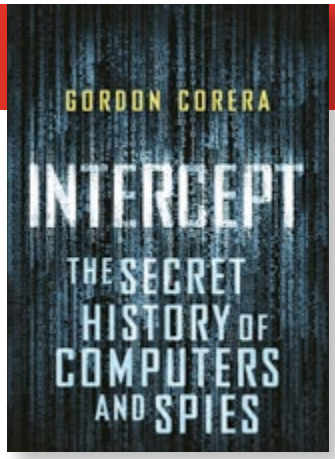
Película:
DEEP WEB

Sinopsis: Deep Web es el documental dirigido por Alex Winter, que recorre todo lo acontecido con el cierre del mercado underground SIlk Road, los bitcoins y la dark web en general.
Cubriendo el juicio de Ross Ulbricht, el documental presenta entrevistas con el escritor de Wired Andy Greenberg y con el programador Amir Taaki.

Película:
DOWNLOADED

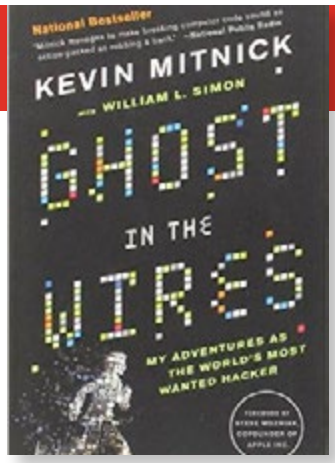
Sinopsis: ¿Recuerdas la primera vez oíste algo sobre Napster? Este documental de Alex Winter trata sobre lo que se conoce como el primer "music hack" que cambió el mundo audiovisual. Este documental recorre la vida de Shawn Fanning y Sean Parker explicando cómo lanzaron Napster en la década de los 90.

Este es un gran documental que muestra cómo una pequeña idea (una piedra en un estanque) creció e impactó a decenas de millones de personas y la industria musical, incluyendo a Lars Ulrich de Metallica, una de las bandas que demandaron a Napster.



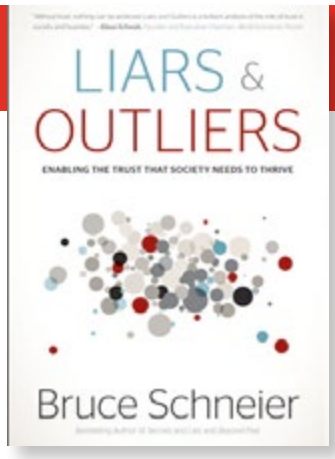
Libro:
INTERCEPT

Autor: Gordon Corera
Num. Paginas: 320
Editorial: W&N
Año: 2015
Precio: 20.00 Euros
Sinopsis: El autor lleva a cabo un repaso histórico del espionaje desde la Segunda Guerra Mundial hasta la era de Internet.



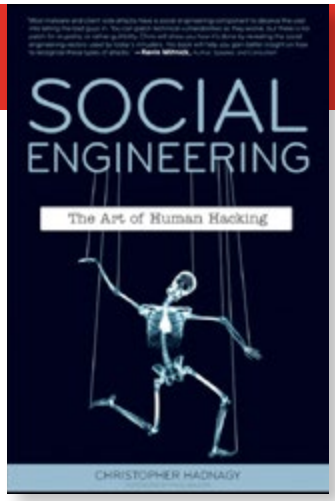
Libro:
GHOST IN THE WIRES

Autor: Kevin Mitnick
Num. Paginas: 520
Editorial: Back Bay
Año: 2012
Precio: 30.00 Euros
Sinopsis: El autor, uno de los hackers más buscados de los Estados Unidos, narra sus aventuras en la red.



Libro:
LIARS & OUTLIERS

Autor: Bruce Schneier
Num. Paginas: 384
Editorial: John Wiley and Sons
Año: 2012
Precio: 25.00 Euros
Sinopsis: El autor reflexiona sobre el binomio confianza y sociedad de la información.



Libro:
SOCIAL ENGINEERING

Autor: Christopher Hadnagy
Num. Paginas: 416
Editorial: John Wiley and Sons
Año: 2010
Precio: 22.00 Euros
Sinopsis: El autor realiza un análisis, desde el punto de vista técnico, de las diferentes formas de ingeniería social.

7.2 Webs recomendadas

www.first.org

www.stopthinkconnect.org

www.cybsecurity.org

www.redseguridad.com

https://ics-cert.us-cert.gov/

www.thiber.org
(NUEVA WEB LANZADA)

www.owasp.org

7.3 Cuentas de Twitter

@ASPI_ICPC

@THIBER

@firstdotorg

@ForbesTech

@cybsecurity_org

@CCNCERT

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
5-8 sept	Dublin	Source	SOURCE Security Conference Dublin	http://www.sourceconference.com/dublin-2015-main/
6-8 sept	Estambul	Octosec	Hacktrick	http://www.hacktrickconf.com/en/
8-10 sept	Kuala Lumpur	ISDF	ISDF2015 - The Second International Conference on Information Security and Digital Forensics	http://sdiwc.net/conferences/isdf2015/
8-10 sept	Sochi, Rusia	ACM	SIN2015 - The 8th International Conference on Security of Information and Networks	http://www.sinconf.org/sin2015/index.php
5-8 sept	Twente, Holanda	Varios	NSPW (New Security Paradigms Workshop)	http://www.nspw.org/2015
9-10 sept	Washington	INSA	Intelligence and National Security Summit	http://www.intelsummit.org/
5-8 sept	Washington	NIST	Cybersecurity Innovation Forum	http://www.fbcinc.com/e/cif/
9-11 sept	Londres	44Con	44CON London	http://44con.com/
14-16 sept	Leon	Universidad de León	I Jornadas Nacionales de Investigación en Ciberseguridad	http://jornadasciberseguridad.riasc.unileon.es/
15-16 sept	Varsovia	Cybersecurity Foundation	SCS 2015: Security Case Study 2015	https://www.securitycasestudy.pl/en/
13-15 Sept	Abu Dhabi	TMC	GCC Cybersecurity Summit 2015	http://www.gcc-cybersecurity.com/

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
15 sept	Barcelona	Usuaria	SEGURINFO Spain 2015	http://www.segurinfo.org/home.php
15-17 sept	Mons, Bélgica	OTAN	NIAS 2015 Cybersecurity Forum	http://nias2015.com/
22 sept	Madrid	DPI / ISMS Forum	VII Foro del Data Privacy Institute	https://www.ismsforum.es/evento/632/vii-foro-de-la-privacidad-del-data-privacy-institute/
22 sept	Campanillas, Málaga	CITIC	Presentación del Capítulo Andaluz de Ciberseguridad	http://www.citic.es/index.php/sala-de-prensa/noticias/703-presentacion-del-capitulo-andaluz-de-la-aei-ciberseguridad-y-de-la-certificacion-de-proveedores-de-ciberseguridad
28-29 sept	Krakovia	The Kosciuszko Institute	CYBERSEC European Cybersecurity Forum	http://cybersecforum.eu/en/
30 sept - 2 Oct	Praga	Virus Bulletin	VB2015	https://www.virusbtn.com/conference/vb2015/index

www.realinstitutoelcano.org
www.blog.rielcano.org
www.globalpresence.realinstitutoelcano.org

www.thiber.org
twitter.com/thiber_esp
linkedin.com/groups/THIBER-the-cybersecurity-think-tank