JULIO 2016 / Nº 16

# 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.

Informe editado en Madrid.

Más información:

**Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.**

**THIBER, The Cyber Security Think Tank.**

# Índice


1 Comentario Ciberelcano .....04

2 Análisis de actualidad internacional .....06

3 Entrevista a Augusto Pérez Arbizu .....11

4 Informes y análisis sobre ciberseguridad publicados en junio de 2016 ..... 16

5 Herramientas del analista .....17

6 Análisis de los ciberataques del mes de junio de 2016 .....20

7 Recomendaciones

7.1 Libros y películas .....28

7.2 Webs recomendadas .....30

7.3 Cuentas de Twitter.....30

8 Eventos.....31

# 1 COMENTARIO CIBERELCANO
## El Brexit y la ciberseguridad

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

Fuente: ComputerWeekly

¿Cómo afectara el Brexit a la ciberseguridad nacional del Reino Unido? Según una encuesta realizada a principios de junio - tres semanas antes de la celebración del referéndum - el 64% de los expertos británicos en ciberseguridad opinaban que el Brexit no tendría consecuencias negativas para la seguridad de su ciberespacio nacional. Sin embargo, tras el referéndum son muchos los analistas británicos y extranjeros que proporcionan una visión más pesimista sobre el futuro de la ciberseguridad del Reino Unido.

Debemos recordar que en los próximos meses se espera que el gobierno británico apruebe y haga pública la segunda Estrategia Nacional de Ciberseguridad que, partiendo de los hitos alcanzados por la primera, aprobada en noviembre de 2011, contará con un presupuesto aproximado de 2.500 millones de euros para consolidar el incipiente Sistema Nacional de Ciberseguridad. Presumiblemente, esta nueva estrategia se verá condicionada por el Brexit pero seguirá girando en torno a los siguientes cuatro grandes objetivos:

- Luchar contra el cibercrimen y convertir al Reino Unido en el lugar más seguro del mundo para hacer negocios en el ciberespacio.

- Mejorar las **cibercapacidades** defensivas del país.

- Trabajar en el desarrollo de un **ciberespacio** lo más abierto y estable posible.

- Generar los conocimientos, habilidades y capacidades que necesita el **Sistema Nacional de Ciberseguridad** del país para su desarrollo.

No cabe duda de que uno de los pilares fundamentales en la lucha contra el cibercrimen es la colaboración internacional y, en especial, la compartición de información entre las Fuerzas y Cuerpos de Seguridad y Servicios de Inteligencia. En este sentido, en enero de 2013 se creaba, en el seno de la EUROPOL, el European CyberCrime Center (EC3) con la misión de coordinar la lucha contra el cibercrimen en el ámbito de la Unión Europea. La salida del Reino Unido de la UE puede ralentizar esta colaboración impactando negativamente en muchas de sus aspiraciones , entre ellas la de ser el "lugar más seguro del mundo para hacer negocios en el ciberespacio".

Del mismo modo, el Reino Unido podría disponer de una legislación propia en materia de protección de datos y comercio electrónico, hasta ahora dictadas desde Bruselas. Este hecho, dependiendo como se gestione, podría incluso ser beneficioso para el Reino Unido.

*"El Brexit impactará en la nueva estrategia británica de ciberseguridad"*

En la actualidad, el Reino Unido no dispone de un número suficiente de expertos nacionales para cubrir sus necesidades en materia de ciberseguridad. Es por ello que el Gobierno británico ha potenciado la educación en el ámbito universitario apoyándose en los **Centros de Excelencia en Ciberseguridad** y la creación de programas de doctorado en esta materia. Se estima que un 30% de los estudiantes de estos centros de excelencia son ciudadanos europeos. Presumiblemente, este porcentaje se vería disminuido por las restricciones inherentes a la ejecución del Brexit. Del mismo modo, la salida del Reino Unido de la Unión Europea podría frenar la contratación de "talento europeo", impactando negativamente en el desarrollo de industria y el sector nacional de ciberseguridad y, por extensión, en la generación de los conocimientos, habilidades y capacidades que necesita el Sistema Nacional de Ciberseguridad Britanico.

En definitiva, no cabe duda de que el Brexit tendrá un impacto sobre la ciberseguridad nacional británica. Es por ello, que el gobierno de Londres deberá llevar un a cabo un análisis pormenorizado de la situación cuyos resultados seguramente impactaran en la redacción y dotación presupuestaria de la futura estrategia nacional de ciberseguridad.

# 2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

## La ciberdefensa aliada

**AUTORA: Clara Rodriguez Chirino.** Analista internacional de THIBER.

La *próxima semana* se celebrará en Varsovia la Cumbre de Jefes de Estado o de Gobierno de la Alianza Atlántica. La agenda del encuentro cubrirá numerosos aspectos de actualidad, la mayoría de ellos relacionados con la Federación Rusa (la creciente asertividad en su área de influencia y el empleo de estrategias híbridas, las relaciones entre la OTAN y Ucrania o el refuerzo de la presencia militar en los países bálticos), el compromiso suscrito en la Cumbre de Gales (2014) de incrementar el gasto en defensa de los veintiocho o la consolidación de la ciberdefensa aliada tres lustros después de que la OTAN tomara conciencia del valor estratégico del ciberespacio. Precisamente, este artículo pretende repasar la evolución de la ciberdefensa aliada desde sus inicios hasta la actualidad.

*"NCIRC es el responsable de prevenir, detectar y responder a los ciberataques que sufre la OTAN"*

La toma de conciencia de la Alianza Atlántica del potencial que posee el ciberespacio para el desarrollo de las operaciones militares se produjo en 1999. Coincidiendo con la Operación Fuerza Aliada en Kosovo y el bombardeo por error de la embajada china en Belgrado, hacktivistas serbios, rusos y chinos realizaron varios ataques de Denegación de Servicio y *defacements* sobre su *sitios web*. Aunque irrelevantes, estos incidentes mediaron para que Bruselas considerara conveniente mejorar la protección de sus redes informáticas, aumentar las capacidades de sus miembros y cooperar con otros actores, especialmente la Unión Europea y el sector industrial.

Sin embargo, fue necesario esperar hasta la Cumbre de Praga (2002) para que la OTAN reconociera el valor intrínseco del ciberespacio. Condicionada por los trágicos sucesos del 11 de Septiembre de 2001 y por el arranque del proceso de *transformación militar*, en la capital checa se tomaron varias iniciativas relevantes para la construcción de una ciberdefensa aliada. No sólo se reconoció la necesidad de incrementar la seguridad de los Sistemas de Información y Comunicaciones de la organización y se lanzó la *NATO Computer Incident Response Capability* (NCIRC) para prevenir, detectar y responder a ciberincidentes; sino que el *Compromiso de Capacidades de Praga* incluyó un paquete de medidas encaminadas a mejorar las cibercapacidades defensivas de la OTAN. Mientras NCIRC logró la plena capacidad operativa en 2014, el Paquete de Capacidades fue implementado

de manera parcial, puesto que muchos países – desconocedores del valor intrínseco del ciberespacio para la seguridad nacional – solamente desarrollaron defensas pasivas.

Aunque la *Guía de Política General* – aprobada por el Consejo del Atlántico Norte en 2005 y refrendada en la Cumbre de Riga de 2006 para llenar el vacío estratégico existente entre los Conceptos Estratégicos de Washington (1999) y Lisboa (2010) – reconocía el valor intrínseco del ciberespacio para la seguridad euroatlántica, no fue hasta los *ciberataques contra Estonia de 2007* cuando la OTAN tomó conciencia de los efectos técnicos y de las implicaciones políticas que podían tener este tipo de incidentes. Estonia quedó paralizada tras una campaña de ataques de Denegación de Servicio Distribuido (DDoS) realizados por hackers rusos, supuestamente coordinados desde el Kremlin. Como resultado, a principios de 2008 la OTAN aprobó el primer *Concepto de Ciberdefensa y la Política de Ciberdefensa*. Avalados en la Cumbre de Bucarest de Abril de 2008, donde se enfatizó *"…la necesidad para la OTAN y las naciones de proteger los sistemas de información claves, compartir las mejores prácticas y proporcionar capacidades para asistir a los países aliados (bajo petición) para contrarrestar un ciberataque".* Además, se desarrollaron los fundamentos de la ciberdefensa aliada con la llamada Ciberdefensa 1.0 y se establecieron tres pilares básicos en esta materia: subsidiariedad (en caso de que no exista una petición previa para asistir al Estado víctima, se aplica el principio de responsabilidad exclusive de cada país soberano), no duplicación (para evitar que los esfuerzos se dupliquen) y seguridad (con el fin de garantizar la confianza mutua). Estas medidas motivaron que la ciberdefensa tuviese su propio espacio en la agenda de la OTAN a partir de la Cumbre de Lisboa de 2010.

En verano de 2008, durante el conflicto ruso-georgiano, se evidenció que los *ciberataques* podían apoyar las operaciones convencionales. Ello medió para que el Concepto Estratégico de la OTAN y la Declaración de la Cumbre de Lisboa de 2010 siguieran consolidando la *ciberdefensa aliada*. Los líderes de la OTAN reconocieron, entonces, que la dimensión cibernética estaría presente en los futuros conflictos, lo que fue determinante a la hora de aumentar las capacidades para detectar, evaluar, prevenir,

defender y recuperarse de ciberataques. Para ello, se desarrolló el Paquete de Capacidades de Lisboa para suplir las brechas más importantes, incluyendo mejoras en el NCIRC. Con el objetivo de asistir a los aliados en materia de protección y respuesta, la OTAN estableció dos Equipos de Reacción Rápida que fuesen capaces de hacer frente a las crisis que atravesase la OTAN, así como de apoyar a las redes nacionales en caso de ser atacadas. Si bien proporcionan una limitada asistencia técnica (ayudando a proteger o restablecer los sistemas y coordinar la respuesta), tienen un fuerte valor político al afianzar el compromiso de la Alianza a la hora de apoyar sus propios sistemas y a los aliados. De esta forma, la OTAN sentaba las bases para integrar plenamente el elemento cibernético en las misiones de defensa colectiva, gestión de crisis y seguridad cooperativa.

Durante esta Cumbre, al Consejo del Atlántico Norte se le asignó la tarea de crear e implementar una política sobre ciberdefensa De este modo, Lisboa supuso la formalización de la llamada Ciberdefensa 2.0, que derivó en la actualización de estructuras (tales como NCIRC), además de propiciar una respuesta de forma conjunta a los nuevos retos que plantea el ámbito virtual. La Cumbre de Lisboa elevó los ciberataques a la categoría que ostentan otro tipo de agresiones: la Política sobre Ciberdefensa contemplaba las ciberamenazas como posible causa de la activación del Artículo 5.

*"Es necesario que los aliados desarrollen capacidades específicas porque difícilmente podrán valerse de los medios propios de la OTAN o aprovecharse de las capacidades del resto de los miembros"*

Más adelante, en 2011, se aprobó la política de la OTAN en materia de ciberdefensa. Un año después, se produjo la integración de la ciberdefensa en el Proceso de Planeamiento de Defensa de la OTAN. Asimismo, la ciberseguridad pasó a ser parte de la *Smart Defence* (iniciativa que supone que los aliados cooperen entre sí para generar, de forma efectiva y económicamente rentable, las modernas capacidades de defensa que la Alianza requiere) en la Cumbre de Chicago (2012). Ese mismo año, como fruto de la fusión de varias agencias de la Alianza, se creó la *NATO Communications and Information Agency* (NCIA) con el fin de apoyar el control, vigilancia e inteligencia de la Organización. Por otro lado, la OTAN llevó a cabo una serie de actualizaciones en el NCIRC. En 2013, la OTAN avocó por mejorar las capacidades cibernéticas a nivel nacional, que deben ser compatibles con las de la OTAN y los demás aliados, además de recordar a los Estados miembros que las capacidades de ciberdefensa de la Alianza cubren las necesidades operativas del Cuartel General, la Estructura de Mandos y sus organismos asociados, estando a disposición de los aliados solo en caso de necesidad.

En 2014, los Ministros de Defensa de la OTAN aprobaron la nueva política sobre ciberdefensa, que está aún siendo implementada. Meses más tarde, durante la Cumbre de Gales (2014), los aliados acordaron que la ciberdefensa es uno

de los principales elementos de la defensa colectiva, además de valorar su importancia para hacer frente a crisis y de cooperar en materia de seguridad. Si bien la OTAN debe centrarse en defender sus propias redes virtuales, los aliados se comprometieron a desarrollar las capacidades necesarias para proteger el ciberespacio a nivel nacional. Asimismo, teniendo en cuenta el compromiso de la OTAN con el cumplimiento del derecho internacional en todos los ámbitos, se determinó que es, por ende, aplicable al ciberespacio. Otro aspecto a destacar de esta Cumbre fue la decisión relativa al Artículo 5 del Tratado acerca de los ataques virtuales y una supuesta respuesta colectiva, que derivaría en una nueva Política de Ciberdefensa conocida como Ciberdefensa 3.0. Al respecto, se acordó que la activación del Artículo 5 en caso de un ataque cibernético contra uno de los miembros de la Organización se decidiría tras examinar cada caso en concreto. Por otro lado, la OTAN acuerda mejorar la cooperación con la industria, la compartición de información y la asistencia mutua entre los aliados, así como el adiestramiento y ejercicios.

Tras la Cumbre, la OTAN reforzó su compromiso con la industria en el ámbito de la ciberseguridad, celebrándose un encuentro entre expertos en esta materia y representantes del sector privado para discutir acerca de las distintas formas de colaboración en la esfera del ciberespacio, durante el que se presentó el *NATO Industry Cyber Partnership* (NICP).

El refuerzo en la cooperación entre la OTAN y la Unión Europea (UE) en materia de ciberseguridad se materializó en febrero de 2016 con el T*echnical Arrangement on Cyber Defence*, que permite el intercambio de información entre los equipos de respuesta rápida. Recientemente, a mediados de junio de 2016, los ministros de defensa de los países miembros acordaron que el ciberespacio sería considerado una dimensión más junto con el aire, el mar y la tierra en la Cumbre de Varsovia. De esta forma, al dotar al ciberespacio de este

rango, la OTAN podrá proteger de manera más eficaz sus misiones y operaciones. No obstante, la OTAN mantiene su postura defensiva y restrictiva, comprometiéndose a actuar de conformidad con el derecho internacional.

Aunque en Varsovia se dará un nuevo impulso a la ciberdefensa aliada, todavía quedan algunas preguntas pendientes en esta materia:

**Homogeneizar las capacidades cibernéticas de los estados miembros:** las capacidades de ciberdefensa aliadas cubren las necesidades operativas del Cuartel General, la Estructura de Mandos y los organismos asociados de la Alianza, estando a disposición de los miembros en caso de necesidad, lo que hace necesario que los mismos aliados desarrollen sus propias capacidades de ciberdefensa. Sin embargo, el nivel de madurez de los miembros en esta materia es heterogénea y proporcional a su capacidad de asimilar la importancia estratégica de esta dimensión. Es por ello que muchos países – siendo un caso paradigmático el nuestro – están afrontado su adaptación al ciberespacio desde la urgencia de quien ha llegado tarde a este dominio, y ello requiere mecanismos ágiles y robustos para llevar a cabo una gestión eficiente y eficaz del cambio. Precisamente, esta misma heterogeneidad en materia de cibercapacidades está provocando que algunas de las principales potencias cibernéticas de la OTAN – Estados Unidos, Reino Unido o Canadá, todas ellas pertenecientes al convenio *FiveEyes* – se muestren reticentes a desvelar todo su arsenal cibernético.

**Definir los límites del Artículo 5:** la Alianza sigue trabajando en la conceptualización de ciberataque y determinar el umbral a partir del cual éste debería ser calificado como una agresión contra un estado miembro y, por tanto, un supuesto contemplado por el Artículo 5. En la pasada ministerial, el Secretario General Jens Stoltenberg declaró que un ciberataque *severo* podría ser constitutivo de una respuesta colectiva, aunque ello no ayuda mucho en resolver este asunto. Del mismo modo, *determinar la atribución* de un ciberataque continúa siendo el principal problema con el que se encuentra la OTAN en este ámbito, puesto que hoy en día no es posible - desde un punto de vista tecnológico - determinar con certeza la procedencia de un ciberataque y la responsabilidad última del mismo. En este sentido, a pesar de que la Alianza está definiendo las opciones de respuesta ante un ciberataque enemigo - cibernética, convencional o la combinación de ambas - cabe preguntarse si un ciberataque presumiblemente llevado a cabo por una potencia adversaria implicaría una respuesta real, y mucho menos colectiva.

En definitiva, a pesar de que la ciberdefensa se ha consolidado definitivamente en la OTAN, son muchos los países miembros que todavía no disponen del mínimo de capacidades para protegerse – y mucho menos responder – en caso de ciberataques. Es necesario que los aliados desarrollen capacidades específicas porque difícilmente podrán valerse de los medios propios de la OTAN o aprovecharse de las capacidades del resto de los miembros, muchos de los cuales reticentes a exponer sus ciberfuerzas.

# 3 Entrevista a Augusto Pérez Arbizu.

## Presidente de IGREA (Iniciativa de Gerentes de Riesgo Españoles Asociados) y Director de Riesgos y Seguros de Telefónica

**1. Como presidente IGREA ¿podría indicarnos cuáles son los principales objetivos de la asociación? ¿Cuál es su ámbito de actuación? ¿Qué es FERMA?**

En primer lugar, creo importante reseñar que los socios de IGREA no son personas físicas, sino empresas o entidades representadas por la persona responsable en cada momento de la gestión de sus riesgos y seguros. Podemos resumir los objetivos de IGREA en tres puntos:

- La potenciación de la gerencia de Riesgos y Seguros como función dentro de las empresas y como profesión.

- Ser órgano de representación de las empresas en su calidad de gestores de riesgos y compradores de seguros, frente a instituciones y Mercado Asegurador.

- Intercambio de experiencias y transmisión de conocimiento entre sus miembros, fomentando y defendiendo las mejores prácticas en relación a las metodologías y sistemas utilizados para la gestión, control, análisis, evaluación y financiación de riesgos.

IGREA es una asociación de carácter privado, independiente, apolítica y sin ánimo de lucro, cuyo ámbito de actuación se rige por la Ley Orgánica que regula el derecho de asociación y sus estatutos. El ámbito geográfico es el territorio del Estado Español.

IGREA
Iniciativa Gerentes de Riesgos Españoles Asociados

FERMA es la federación europea de asociaciones de gerentes de riesgos, a la cual pertenece IGREA.

**2. Hemos asistido en los últimos tiempos a un uso incremental y cada vez más sofisticado de los medios digitales en las organizaciones. Hasta hace relativamente poco, los riesgos derivados de esa digitalización del mundo empresarial no se solían transferir al sector asegurador ¿qué es lo que ha cambiado? ¿Son las compañías conscientes de los riesgos tecnológicos a los que tendrán que enfrentarse?**

Pues primero, fue la falta de oferta aseguradora lo que hacía que no se asegurasen estos riesgos. Algunos asegurados, los compradores de seguros más sofisticados, reclamaban soluciones que el Mercado no era capaz de ofrecer.

Sin embargo, aunque la capacidad aseguradora ya existe, ahora es la demanda la que se está haciendo esperar en mercados como el español (en EEUU la demanda despegó ya hace tiempo). Salvo algunas empresas o actividades concretas (operadoras de telecomunicaciones, bancos…), las empresas aún no compran esta cobertura de manera generalizada.

Desde luego en Telefónica sí que somos conscientes de los riesgos tecnológicos. Es por ello, que pusimos en marcha un Programa Multinacional de Seguro para Ciber Riesgos en el año 2008, cuando la oferta aseguradora aún era muy inmadura y casi inexistente.

Es posible, no obstante, que a nivel general las empresas en España si estén tardando algo más en ser conscientes de ello y una vez que lo son, estén tardando también en adoptar soluciones de transferencia de riesgo. Lo que no me cabe duda es que la tendencia es imparable. En pocos años será tan común tener un seguro para Ciber Riesgos como el seguro de incendios o de responsabilidad civil.

**3. En su opinión, ¿el mercado asegurador nacional es lo suficientemente maduro como para ofrecer capacidad ante los riesgos derivados de las ciberamenazas?**

Más que de Mercado Nacional, creo que debemos hablar de Mercado Europeo, dada la posibilidad que existe para cualquier Entidad Aseguradora de operar en todo el territorio de la UE. Dentro del espacio europeo se encuentra Londres, donde tenemos uno de los Mercados de Seguros más maduros y sofisticados del mundo.

Los fundamentos del Seguro se basan en la experiencia y en la estadística. Cuando aparecen riesgos emergentes, donde aún no hay suficiente experiencia acumulada, lleva un tiempo al Mercado empezar a ofrecer soluciones. El problema se agrava si además es un riesgo que evoluciona tan rápido como en este caso.

No obstante, podemos afirmar que existe ya cierta madurez del Mercado para ofrecer capacidad para estos riesgos. Los aseguradores dieron el paso hace ya unos años. La dependencia cada vez mayor de activos digitales (redes, software, sistemas, datos….), ha hecho que los seguros tradicionales, asociados fundamentalmente a activos materiales, pierdan relevancia en las Organizaciones como instrumentos de transferencia de riesgos. Por lo tanto, el Mercado Asegurador se ha visto obligado a adaptarse a este nuevo entorno proponiendo soluciones a los nuevos riesgos tecnológicos. De otra manera se verían abocados a tener un papel muy marginal como solución para la financiación de los riesgos de las empresas.

*"Risks Managers y CISOs deben aliarse y defender conjuntamente frente a la alta dirección la necesidad de poner en marcha coberturas ante ciberamenazas"*

**4. Desde el punto de vista de un Gestor de Riesgos de una gran corporación, y habida cuenta de que cada modelo organizativo presenta sus peculiaridades ¿cómo es la relación con los responsables de seguridad (CISO) y los Responsables de Riesgos? ¿Quién es el responsable de la gestión de los ciber-riesgos y su posterior traspaso al sector asegurador?**

Es posible que una de las barreras para que la demanda despegue en España sea precisamente que la relación entre Risk Manager y CISO en ocasiones no es muy fluida.

El Risk Manager es el especialista en Seguros y conocedor del Mercado. Asimismo, puede llegar a entender bien las consecuencias financieras de los Ciber Riesgos (pérdidas de ingresos, reclamaciones de terceros, daño reputacional….). Sin embargo, el papel del CISO también es clave para completar el análisis y evaluación. Será imprescindible su participación para aportar información de suscripción necesaria para las aseguradoras y "venderles" la gestión que se hace de este riesgo en la Empresa.

En mi opinión, Risk Manager y CISO deben aliarse y defender conjuntamente frente a la alta dirección la necesidad de poner en marcha este tipo de coberturas.

Por último, me gustaría añadir, que si bien estas dos funciones tienen un papel muy relevante en la gestión y transferencia de este riesgo, la responsabilidad debe tener un ámbito transversal en las empresas. No olvidemos que no solo es una cuestión de sistemas, sino también de cultura y comportamiento organizacional. Debe haber concienciación en todos los empleados de la Compañía, respecto a la sensibilidad y confidencialidad de los datos que se manejan. También de cómo reaccionar ante la recepción de determinados correos electrónicos u otro tipo de amenazas. Por este motivo, otras áreas como Auditoría, Cumplimiento o Legal, también tienen bastante que aportar para conseguir una gestión integral de este riesgo.

**5. ¿Cree necesario algún tipo acción proactiva desde el Gobierno para favorecer la adopción de este tipo de productos?**

En mi opinión, los Gobiernos quizás utilizan en exceso la vía sancionadora, como ya vemos en materia de protección de datos. Una empresa que sufre un ataque, normalmente ya tiene bastante con las posibles pérdidas de ingresos, gastos de recuperación de datos, compensaciones a clientes y daño reputacional, como para que encima le puede caer una multa importante. Esto último debería dejarse exclusivamente para casos de incumplimiento de normativas claros o para negligencias graves. Si la Compañías afectadas perciben que al comunicar una fuga de información a la Administración, más que una ayuda, van a recibir un castigo, pues no se fomentará que estos casos salgan a la luz y podamos aprender de ellos y mejorar colectivamente en la lucha contra el ciber crimen.

Pienso que es más interesante balancear la situación hacia una política menos sancionadora y más proactiva en la adopción de este tipo de Pólizas de seguros. Por ejemplo, legislando la obligatoriedad de comprar este seguro en determinados sectores de actividad, como ya se hace con otro tipo de seguros, o bien exigiéndolos en los pliegos de licitación de contratos con la Administración para determinados productos o servicios. Con ello, se consigue un doble objetivo. En primer lugar, se estarán garantizando unos mínimos estándares de seguridad que vienen exigiendo los aseguradores para suscribir este tipo de riesgos. En segundo lugar, una vez producido el siniestro, se tendrá una protección financiera que podrá garantizar la continuidad de la empresa y proteger también a sus clientes finales, con lo cual también se protege el derecho de los consumidores.

Al ser comunicados todos los siniestros a los aseguradores, se generará una base de conocimiento que permitirá un salto cualitativo importante en la lucha contra el ciber crimen, tanto a nivel reactivo como preventivo.

**6. Parece claro el acercamiento entre el sector asegurador y el sector de la ciberseguridad. Algunos analistas vaticinan, como ya ha sucedido en otros ámbitos, una presencia de mayor relevancia de las aseguradoras en la cadena de valor de la ciberseguridad, a través de la adquisición de empresas o participaciones en las mismas. ¿Cree que a medio plazo presenciaremos este hecho?**

Efectivamente hay evidentes sinergias entre ambos sectores. Hay que tener en cuenta la constante evolución del ciber crimen y lo sofisticados que pueden llegar a ser sus ataques, tanto desde el punto de vista tecnológico como de ingeniería social. La mayoría de las empresas, cuando sufren un gran siniestro de estas características tienen grandes limitaciones para reaccionar, por falta de conocimientos y recursos. Por lo tanto, buscan de su asegurador no una mera indemnización económica, sino que les puedan garantizar un servicio 24x7 de recursos de consultoría, forensic, recuperación de datos, etc…

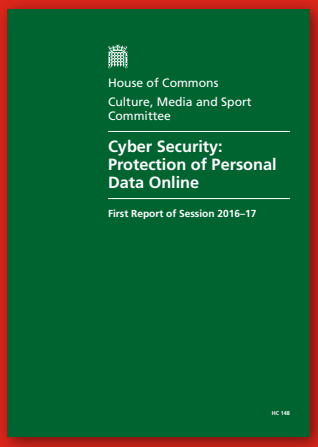
Adicionalmente a los servicios reactivos, el sector de ciberseguridad puede aportar a los aseguradores las capacidades que necesita para suscripción de riesgos, e incluso porque no, paquetizar con el seguro los servicios preventivos que garanticen los mínimos estándares de seguridad de sus asegurados.

Por todo ello, no es extraño que algunas aseguradoras hayan iniciado pasos hacia una integración vertical. Tenemos ejemplos de otros ramos donde esta estrategia se ha consolidado, como en el caso de los seguros de salud, donde algunas aseguradoras son dueñas de grupos de hospitales. Veremos si esta tendencia se consolida también en el caso de los seguros para los riesgos tecnológicos.

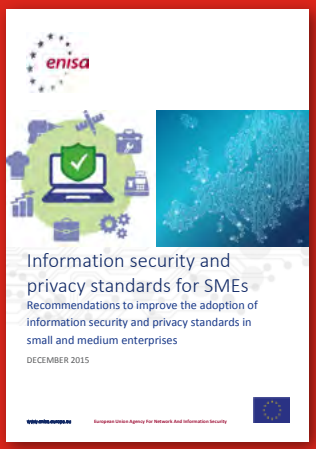
*"…no es de extrañar que algunas aseguradoras hayan iniciado el acercamiento hacia una integración vertical de la oferta ante riesgos tecnológicos"*

# 4 Informes y análisis sobre ciberseguridad publicados en junio de 2016

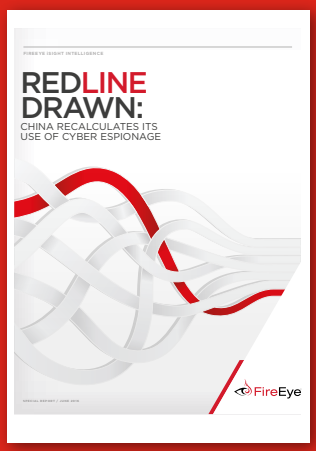
## Cyber Security: Protection of Personal Data Online (UK Government)




## Information Security and Privacy Standards for SMEs (ENISA)



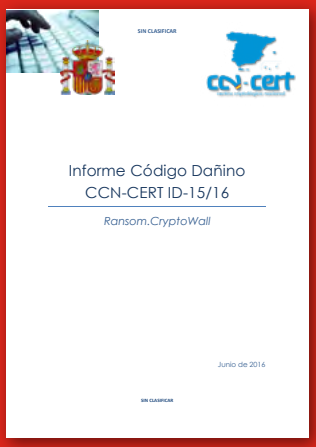

## Redline Drawn: China recalculates its use of cyber espionage (Fireeye)




## The anatomy of Cyber-Jihad (ICIT)

## Analysis of standards related to Trust Service Providers (ENISA)

## Informe Código Dañino: Ransom. Cryptowall (CCN-CERT)




## Estudio sobre la Ciberseguridad y Confianza en los hogares españoles 2016 (ONTSI)

## Guidance on cyber resilience for financial market infrastructures (Bank for International Settlements)

# 5 HERRAMIENTAS DEL ANALISTA: Shodan

Shodan es un motor de búsqueda en internet que permite al analista encontrar tipos específicos de equipos (routers, servidores, dispositivos de toda índole, etc.) conectados a Internet a través de una variedad de filtros. Algunos también lo han descrito como un motor de búsqueda de banners de servicios, metadatos que el servidor envía de vuelta al cliente que lo consulta. Esta información puede ser sobre el software instalado en el servidor, qué opciones admite el servicio, un mensaje de bienvenida o cualquier otra cosa que el cliente pueda saber antes de interactuar con el servicio.

Esta herramienta tiene la particularidad de indexar resultados de manera diferente a los buscadores habituales: en lugar de mostrar contenidos como fotografías, videos, frases y texto, Shodan recorre el rango de direcciones *IP 0.0.0.0/0* y procede a realizar una conexión a los puertos. Es decir, tal como si hiciera un barrido con nmap, muestra lo que no es visible en un sitio web, recurriendo a algo más técnico como un banner grabbing con el cual obtiene **información específica** de un servidor.

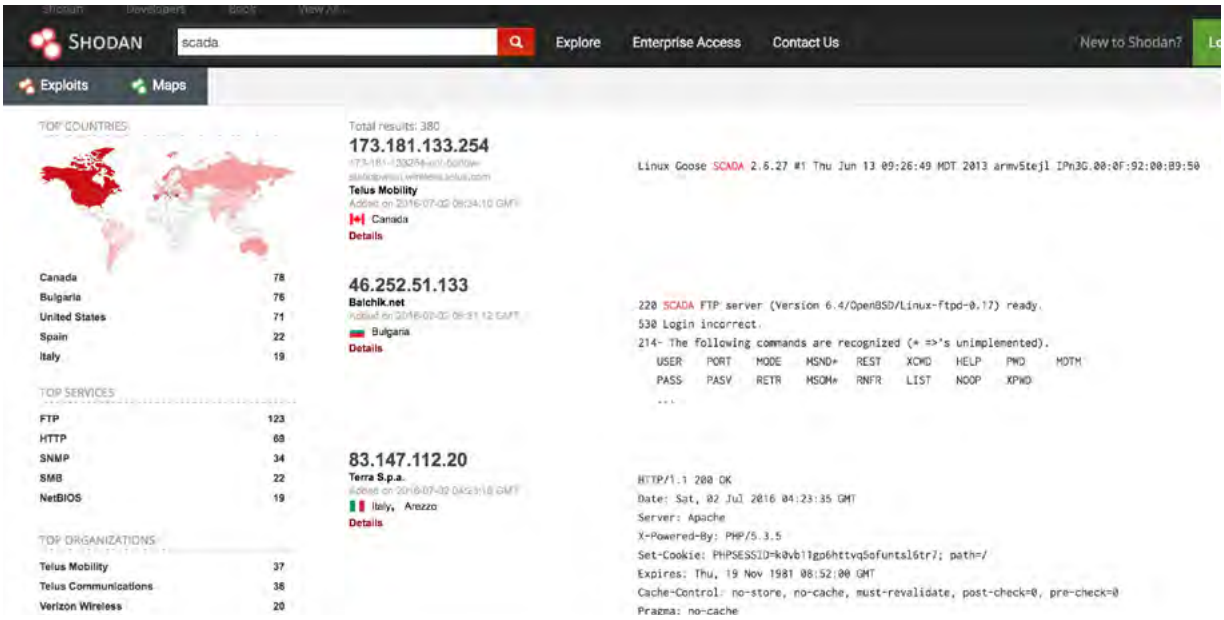



Ilustración: Ejemplo de búsqueda simple en Shodan

Para hacer uso de este buscador es necesario crear una cuenta personal gratuita (también tiene versión de pago), con la cual se tiene acceso a un número limitado de 100 resultados por búsqueda. Si bien puede parecer un número pequeño, se puede obtener muchísima información.

Además, el registro gratuito permite aplicar filtros, como:

- **Country:** permite encapsular la búsqueda solamente a un país especifico, por ejemplo: country:es VOIP

- **City:** Filtro por ciudad, Ejemplo para buscar Servidores Apache en Madrid: city:Madrid Apache

- **port:** Permite hacer búsquedas dependiendo del puerto que tenga abierto o el servicio que se esté ejecutando, ejemplo: port:21 city:Sevilla

- **net:** Para buscar una IP especifica o rangos de IP, ejemplo: net:186.65.127.0/24

- **hostname:** Busca el texto que le indiquemos en la parte de hostname, veamos el resultado de este ejemplo: hostname:Prensa

Shodan recoge datos sobre todo en los servidores web al momento (HTTP puerto 80), pero también hay algunos datos de FTP (21), SSH (22) Telnet (23), SNMP (161) y SIP (5060)

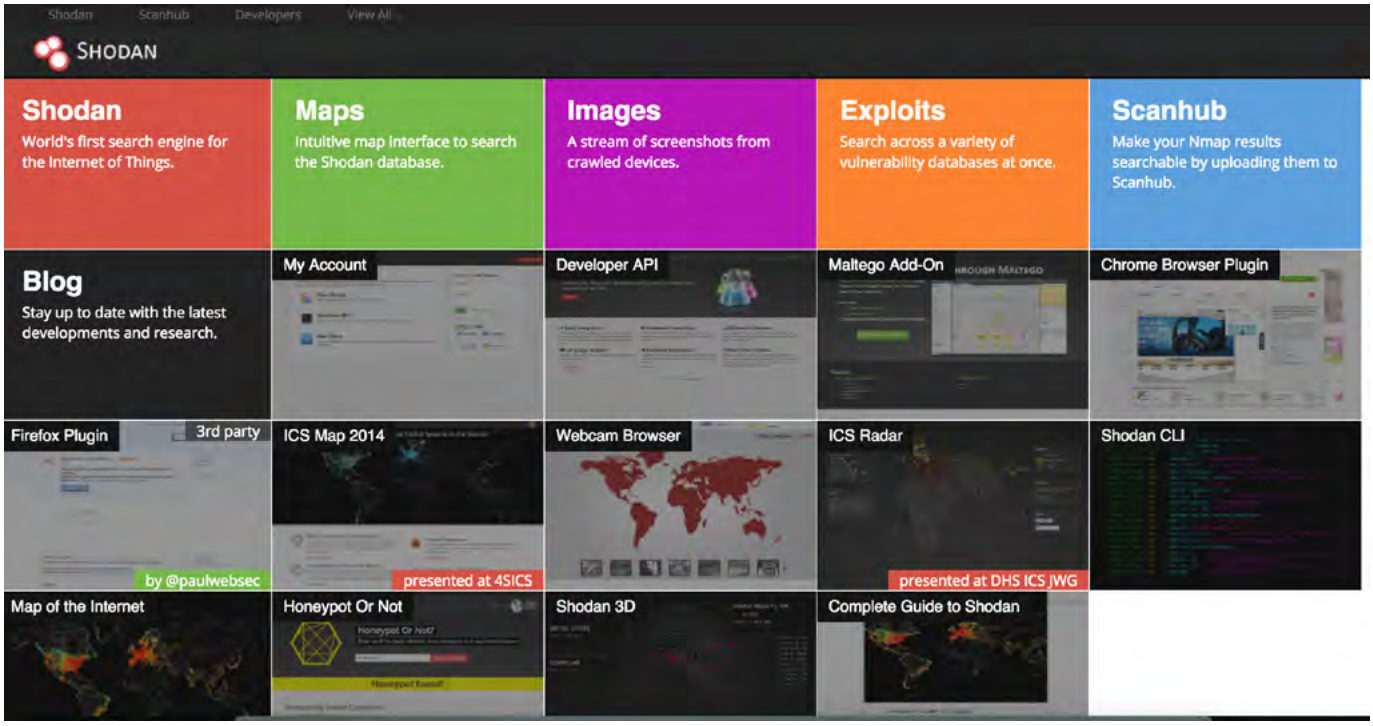



Ilustración Principales funcionalidades disponibles en el portal de Shodan

Shodan obtiene información de unos 500 millones de dispositivos conectados a Internet cada mes. Desde cámaras de seguridad, aires acondicionados, pasando por puertas de cocheras, sistemas VoIP, sistemas de calefacción, plantas de energía y sistemas de automatización industriales.

La herramienta fue lanzada en 2009 por el informático John Matherly, quien, en 2003, concibió la idea de buscar dispositivos vinculados a Internet. El nombre Shodan es una referencia a *SHODAN*, un personaje de la serie de videojuegos *System Shock.*

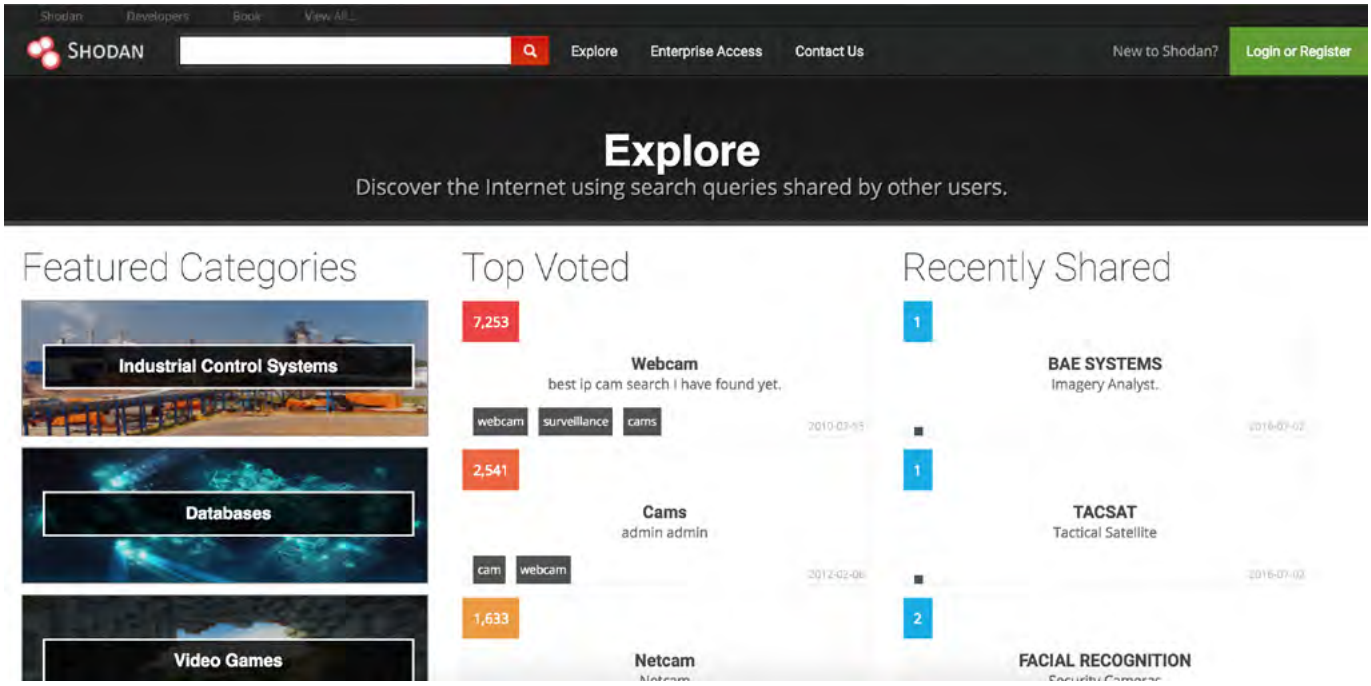



Ilustración  Algunas búsquedas categorizadas en Shodan

# 6 Análisis de los Ciberataques del mes de junio de 2016

**AUTOR: Adolfo Hernández,** subdirector de THIBER, the cybersecurity think tank.
Cybersecurity advisor, Telefonica/ElevenPaths.

## CIBERCRIMEN

Siguiendo con la tendencia predominante en los últimos meses, de nuevo durante este periodo se han vuelto a registrar dos grandes fugas de datos de credenciales de usuario.

El 26 de mayo de 2016 se anunciaba la venta de una fuga de información de 427.484.128 contraseñas filtradas pertenecientes a un total de 360 millones de usuarios de MySpace. Según *LeakedSource* las contraseñas les han sido facilitadas por un usuario que responde al nombre de Tessa88@exploit.im / Peace.

Aparentemente es una mujer de origen Ruso, y su nickname ha sido asociado a la puesta en venta de los datos filtrados de Twitter, VK y LinkedIn, entre otros.

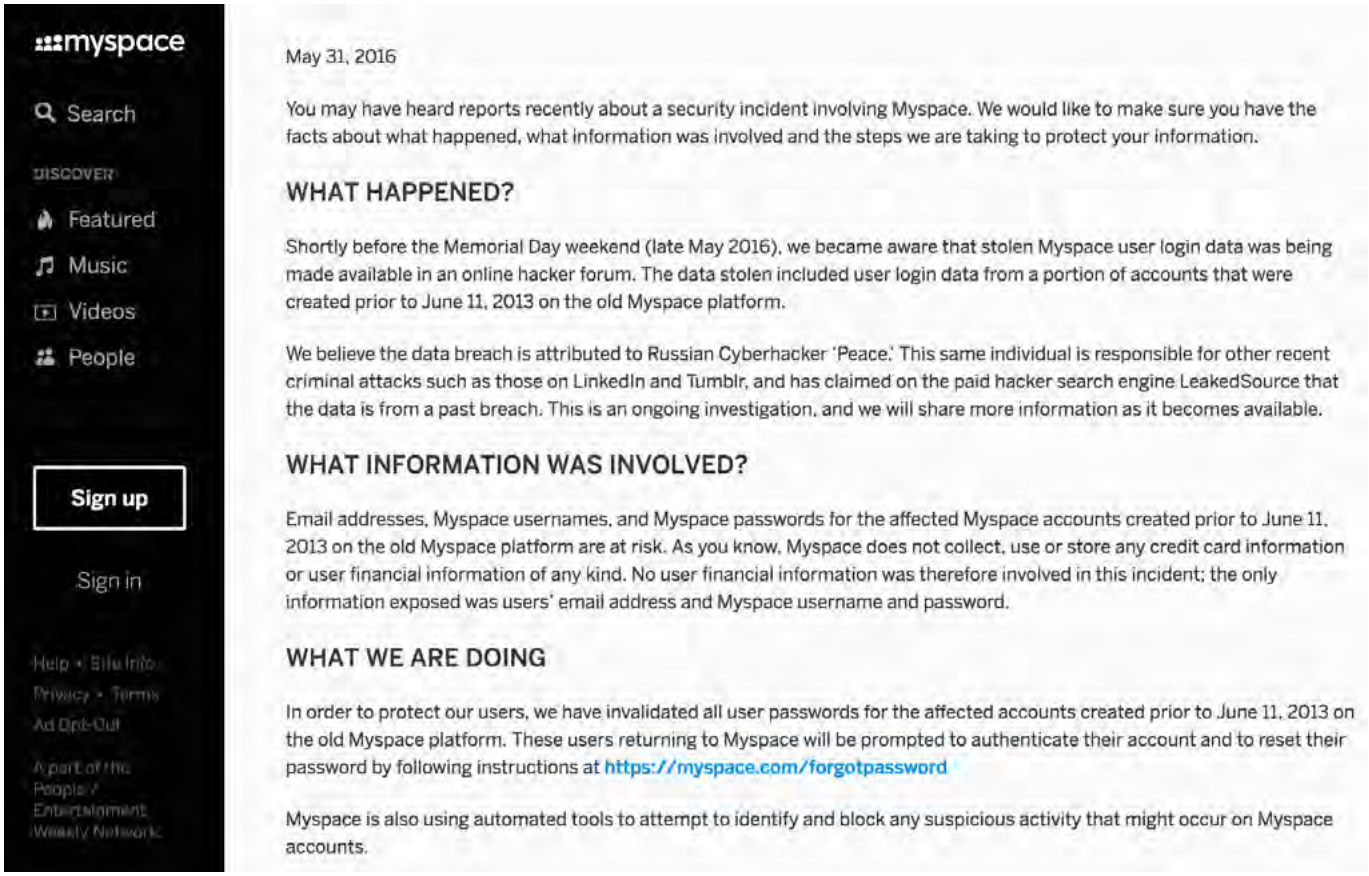
*Peace puso a la venta la información en un foro de la deep web y pidiendo 6 Bitcoins (aproximadamente $2.800)* por la base de datos de correos electrónicos y contraseñas. La filtración de datos podría haberse producido en un marco temporal comprendido desde finales de 2008 hasta principios de 2009.

Las credenciales, al parecer, estaban almacenadas en un servidor protegido con SHA1 sin Salt, un algoritmo cuyo uso es considerado inseguro por un número creciente de profesionales de la comunidad de la ciberseguridad.

| Rank | Password | Frequency |
|---|---|---|
| 1 | homelesspa | 855,478 |
| 2 | password1 | 585,503 |
| 3 | abc123 | 569,825 |
| 4 | 123456 | 487,945 |
| 5 | myspace1 | 276,915 |
| 6 | 123456a | 244,641 |
| 7 | 123456789 | 191,016 |
| 8 | a123456 | 165,132 |
| 9 | 123abc | 159,700 |
| 10 | (POSSIBLY INVALID) | 158,462 |
| 11 | qwerty1 | 141,110 |
| 12 | passer2009 | 130,740 |
| 13 | fuckyou1 | 125,302 |
| 14 | iloveyou1 | 123,668 |
| 15 | princess1 | 114,107 |
| 16 | 12345a | 111,818 |
| 17 | monkey1 | 106,424 |
| 18 | football1 | 101,149 |
| 19 | babygirl1 | 90,685 |
| 20 | love123 | 88,756 |

Ilustración. Análisis de las contraseñas de MySpace más utilizadas entre las cuentas filtradas

La poca popularidad de MySpace hace que el peligro del robo no esté en que alguien pueda entrar a los perfiles de los usuarios, sino en que se utilicen los emails para intentar acceder a otros espacios de mayor importancia, como los buzones de correo o las cuentas de entidades bancarias.



myspace

Search

DISCOVER

Featured

Music

Videos

People

Sign up

Sign in

May 31, 2016

You may have heard reports recently about a security incident involving Myspace. We would like to make sure you have the facts about what happened, what information was involved and the steps we are taking to protect your information.

WHAT HAPPENED?

Shortly before the Memorial Day weekend (late May 2016), we became aware that stolen Myspace user login data was being made available in an online hacker forum. The data stolen included user login data from a portion of accounts that were created prior to June 11, 2013 on the old Myspace platform.

We believe the data breach is attributed to Russian Cyberhacker 'Peace.' This same individual is responsible for other recent criminal attacks such as those on LinkedIn and Tumblr, and has claimed on the paid hacker search engine LeakedSource that the data is from a past breach. This is an ongoing investigation, and we will share more information as it becomes available.

WHAT INFORMATION WAS INVOLVED?

Email addresses, Myspace usernames, and Myspace passwords for the affected Myspace accounts created prior to June 11, 2013 on the old Myspace platform are at risk. As you know, Myspace does not collect, use or store any credit card information or user financial information of any kind. No user financial information was therefore involved in this incident; the only information exposed was users' email address and Myspace username and password.

WHAT WE ARE DOING

In order to protect our users, we have invalidated all user passwords for the affected accounts created prior to June 11, 2013 on the old Myspace platform. These users returning to Myspace will be prompted to authenticate their account and to reset their password by following instructions at https://myspace.com/forgotpassword

Myspace is also using automated tools to attempt to identify and block any suspicious activity that might occur on Myspace accounts.

Ilustración. Notificación oficial del incidente en la página de myspace

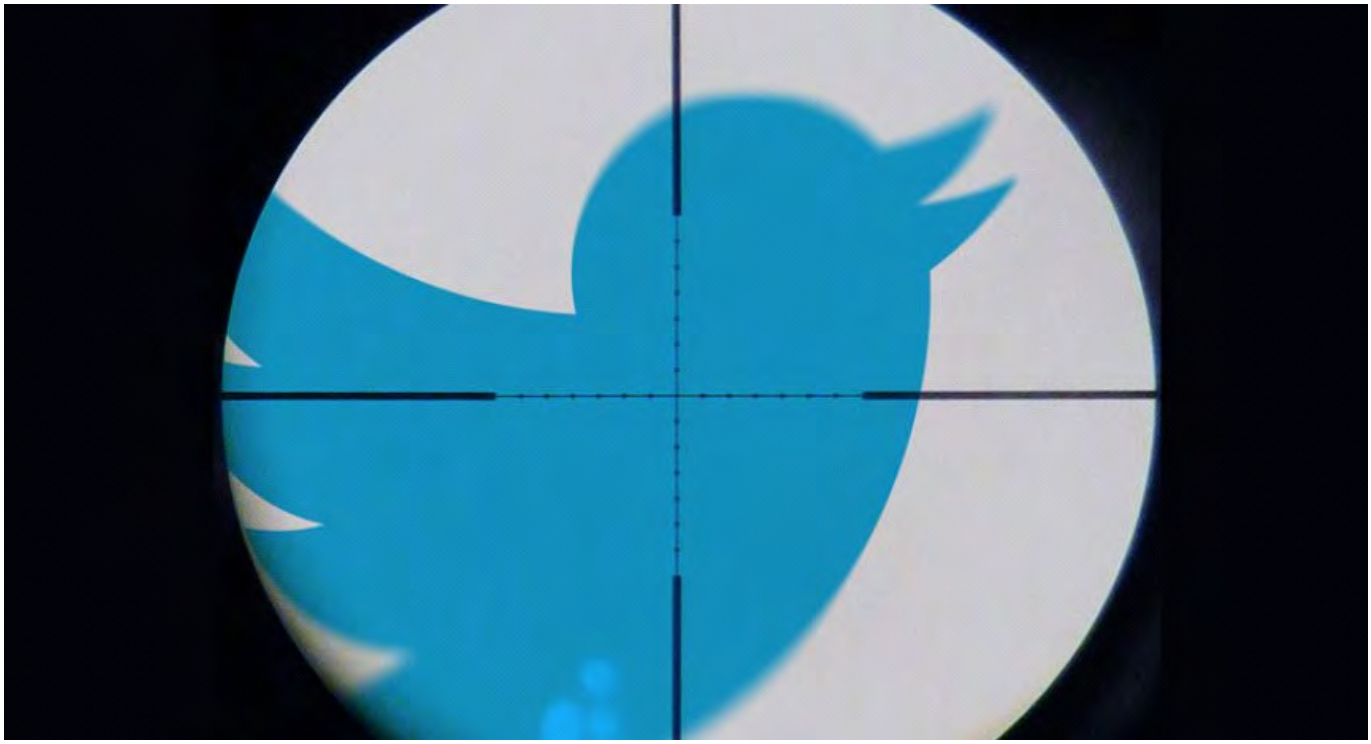
Por otra parte, a mediados de mes, unos cibercriminales de habla rusa pusieron a la venta credenciales de usuario, contraseñas y otros detalles de cerca de 3.488 servidores comprometidos en la India por 6 $ la unidad en diversos foros en la Deep web, *según afirma Kaspersky en un informe publicado por su equipo de analistas.*

La plataforma de comercio online dedicada a la compraventa de información filtrada y servicios de seguridad ofensivos *xDedic* identificó a un grupo de habla rusa que afirmaba contar actualmente con 70.624 servidores comprometidos poniéndolos a la venta con control total y acceso remoto a través de Remote Desktop (RDP).

En el propio informe de Kaspersky, se menciona que la India ocupa el cuarto lugar en cuanto a servidores hackeados con cerca de 3.488 servidores comprometidos que aparecen en xDedic desde comienzos de 2016. Además, muchos de los servidores puestos a la venta durante el mes de mayo y junio son servidores web que albergan sitios populares, programas de contabilidad financiera, servidores de correo y de software de Punto de Venta (POS).

El acceso a esos servidores puede ser utilizado para atacar el resto de la infraestructura TI de los propietarios legítimos o como una plataforma de lanzamiento para ataques más amplios, mientras que los propietarios, que incluyen entidades gubernamentales, empresas y universidades, desconocen el estado de compromiso de sus servidores.

Finalmente, el 21 del mes pasado, *LeakedSource*, se hizo eco de una filtración pública de credenciales de usuarios de Twitter, cuya fuente es, a su vez, un usuario autodenominado Tessa88@exploit.im, el mismo alias utilizado para anunciar que había sido asaltada la red social rusa VK y que estaban en el aire los datos de más de 100 millones de usuarios.



En este caso, la fuga afecta a un total de 41 millones de credenciales pertenecientes a cuentas de Twitter. Los datos filtrados se recogían en un único fichero en el que aparecían en cada línea el nombre de usuario o correo electrónico y la contraseña asociada en claro. 32 millones de esas credenciales aparecieron a la venta en varios marketplaces de la Deep web.

Es este último aspecto el que ha hecho que *la empresa que dirige Jack Dorsey niegue* que los datos hayan sido obtenidos tras un asalto a sus servidores o por una fuga de datos de la compañía, lo que apunta a que los atacantes hayan usado algún tipo de malware o campañas de ingeniería social (como el pishing) para obtener directamente las credenciales de los usuarios finales.

Leakedsource explica en una entrada de su blog cómo cualquier usuario puede entrar a comprobar si su nombre y contraseña se encuentra entre los 32.888.300 datos de Twitter que han sido puestos en circulación. Adicionalmente, también explica que los datos de Mark Zuckerberg, el fundador de Facebook, no están entre ellos.

Al mismo tiempo, esta publicación ha permitido hacer un análisis de las contraseñas más utilizadas entre esos 41 millones de usuarios.

| POSICIÓN | CONTRASEÑA | NÚMERO DE VECES USADA |
|---|---|---|
| 1 | 123456 | 120.417 |
| 2 | 123456789 | 32.775 |
| 3 | qwerty | 22.770 |
| 4 | password | 17.471 |
| 5 | 1234567 | 14.401 |
| 6 | 1234567890 | 13.799 |
| 7 | 12345678 | 13.380 |
| 8 | 123321 | 13.161 |
| 9 | 111111 | 12.138 |
| 10 | 12345 | 11.239 |

Ilustración 3 Análisis de las contraseñas de Twitter más utilizadas

## CIBERESPIONAJE

Durante este mes, se ha conocido que Corea del Norte atacó más de 140.000 ordenadores en 160 empresas y agencias gubernamentales de Corea del Sur, inyectando código malicioso en los mismos en una operación a largo plazo para lanzar, aparentemente, un ataque cibernético masivo contra su rival, según han confirmado fuentes policiales surcoreanas.

Corea del Sur ha estado en alerta máxima contra ciberataques por parte de su vecino del norte después de que el régimen de Pyongyang llevase a cabo una prueba nuclear en enero y el lanzamiento de un cohete de largo alcance en febrero que condujo a nuevas sanciones por parte de la ONU.

El origen de esta campaña de ataques se remonta a 2014 y fueron detectados en febrero de este año, después de que Corea del Norte lograse hacerse con la información de dos conglomerados empresariales relacionados con el sector de la defensa.

Se ha detectado presencia norcoreana en muchos de los servidores comprometidos, sin detectarse actividad maliciosa en los mismos tras el acceso inicial, lo que aumenta las sospechas de la intención de lanzar un ataque a gran escala a medio o largo plazo o, simplemente, hacerse con secretos industriales y militares.

Por otra parte, *hackers rusos apararentemente asociados a actores gubernamentales de su país, consiguieron acceder la red informática del Comité Nacional Demócrata* (DNC por sus siglas en inglés) y tuvieron acceso a toda la base de datos de la investigación de la oposición del candidato presidencial republicano Donald Trump, según afirman funcionarios del comité de seguridad demócrata y diversas firmas de seguridad norteamericanas.

El ataque otorgó visibilidad a los usuarios externos durante más de un año a las bases de datos del sistema, al correo electrónico y al tráfico de los sistemas de mensajería.

Del mismo modo, otros sistemas informáticos que sustentan la campaña de los candidatos presidenciales Hillary Clinton y Donald Trump también fueron blanco de ataques de potencial origen ruso, según han comentado algunos expertos al Washington Post, sin embargo no aportan detalles sobre estos incidentes.

Como era de esperar, un portavoz de la embajada de Rusia dijo que no tenía conocimiento de tales intrusiones y Dmitry Peskov, portavoz del Kremlin, notificó a la agencia de noticias Reuters en Moscú que ningún agente estatal ruso se encontraba tras estos ataques.

Por su parte, el DNC ha notificado públicamente que ningún dato de carácter financiero, de donaciones o información personal parece haber sido filtrado, lo que sugiere que la brecha era el resultado de una acción de espionaje tradicional, no el trabajo de un grupo de ciberatacantes aislado.

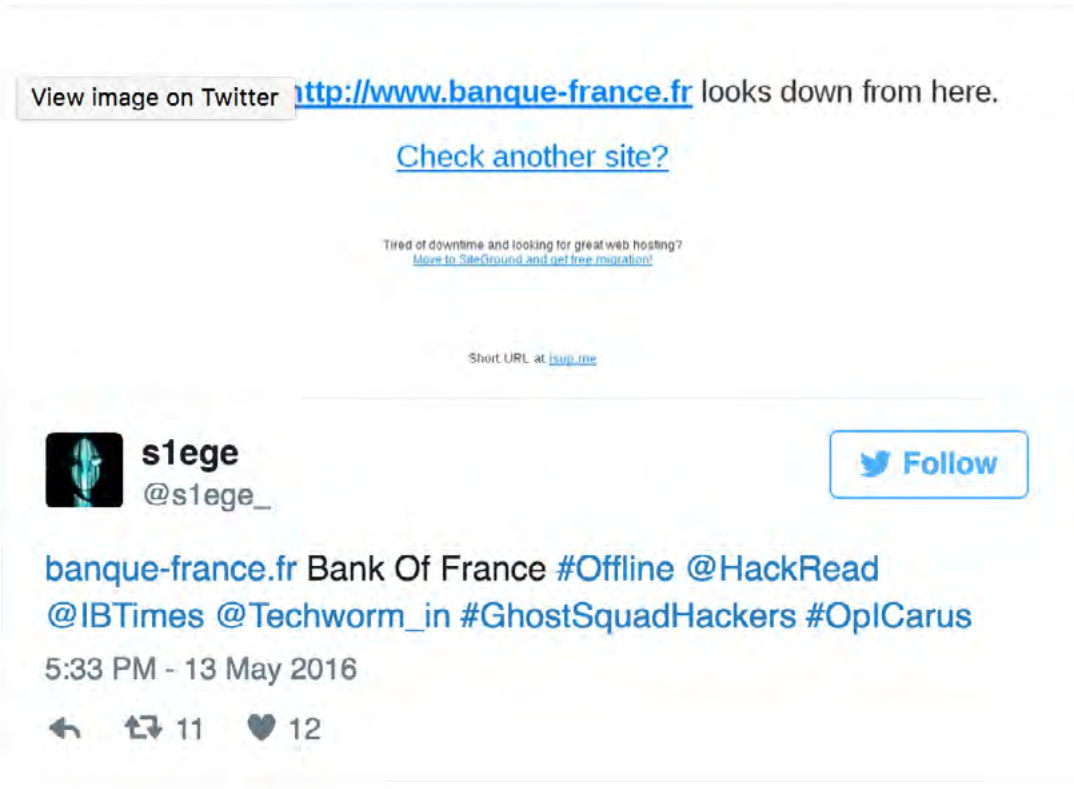
Estas intrusiones son un ejemplo del interés de Rusia en el sistema político estadounidense y su deseo de entender las políticas, las fortalezas y debilidades de un potencial futuro presidente.

La profundidad y persistencia del ataque refleja la habilidad y la determinación de un adversario de EEUU en el entorno cibernético como Rusia, focalizando muchos de sus ataques sobre objetivos estratégicos como la Casa Blanca, el Dpto. de Estado y las organizaciones asociadas a la camapaña política en la que se encuentra el país.

## HACKTIVISMO

En el plano del hacktivismo, un grupo asociado a Anonymous continúa con una campaña desde principios de mes contra diversas instituciones financieras internacionales, ejecutando ataques de denegación de servicio distribuido. El colectivo hacktivista comenzó atacando dieciocho bancos entre el 13 y el 19 de mayo. Entre las entidades afectadas se encuentran la bolsa de Nueva York, Royal Bank of Scotland, Banco de Francia, y cinco sucursales diferentes de la Reserva Federal de Estados Unidos.

La autoría fue reclamada por a través de diversos tuits desde las cuentas de Twitter de S1ege y Scrub. La cuenta de Twitter de Ghost Squad - un subgrupo afiliado a Anonymous - también publicó varios tuits que corroboraron los ataques.

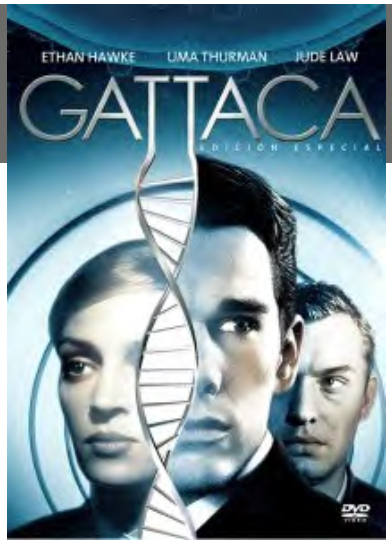


Cada uno de las webs de los bancos atacados parecen haber estado caídas por un período de tiempo diferente. Mientras que la bolsa de valores de Nueva York estuvo caída durante cuatro horas, el Union Bank de Camerún estuvo inaccesible durante 48 horas.

No existe información detallada sobre las pérdidas asociadas a los ataques, pero los ataques se han sucedido desde mediados de mayo durante todo el mes de junio.

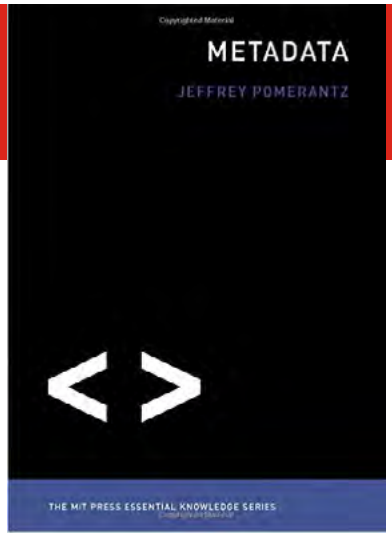
# 7 Recomendaciones

## 8.1 Libros y películas



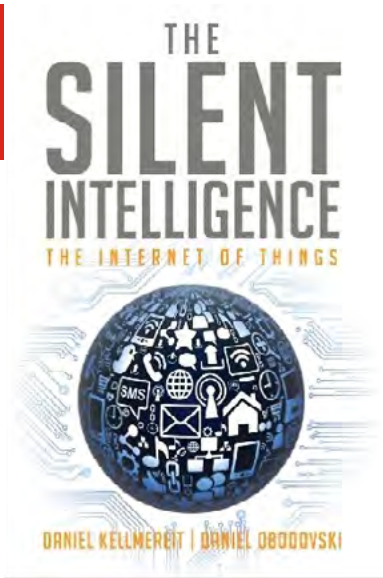

**Película:**
**GATTACA**

**Sinopsis:** Ambientada en una sociedad futura, en la que la mayor parte de los niños son concebidos in vitro y con técnicas de selección genética. Vincent, uno de los últimos niños concebidos de modo natural, nace con una deficiencia cardíaca y no le auguran más de treinta años de vida. Se le considera un inválido y, como tal, está condenado a realizar los trabajos más desagradables. Su hermano Anton, en cambio, ha recibido una espléndida herencia genética que le garantiza múltiples oportunidades. Desde niño, Vincent sueña con viajar al espacio, pero sabe muy bien que nunca será seleccionado. Durante años ejerce toda clase de trabajos hasta que un día conoce a un hombre que le proporciona la clave para formar parte de la élite: suplantar a Jerome, un deportista que se quedó paralítico por culpa de un accidente. De este modo, Vincent ingresa en la Corporación Gattaca, una industria aeroespacial, que lo selecciona para realizar una misión en Titán. Todo irá bien, gracias a la ayuda de Jerome, hasta que el director del proyecto es asesinado y la consiguiente investigación pone en peligro los planes de Vincent.



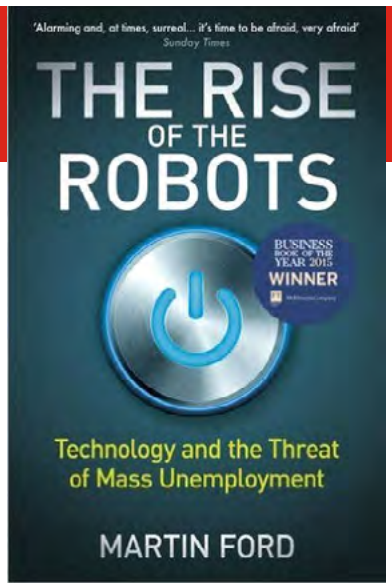

**Libro:**
**METADATA**

**Autor:** Jeffrey Pomerantz
**Num. Páginas:** 256
**Editorial:** MIT Press
**Año:** 2015
**Precio:** 25.00 Euros
**Sinopsis:** Tras las revelaciones de Edward Snowden, el concepto METADATO ha dejado de ser anónimo para buena parte de la opinión pública. De la mano del MIT, este libro analiza como los metadatos son un elemento clave para comprender la evolución de las sociedades del futuro.



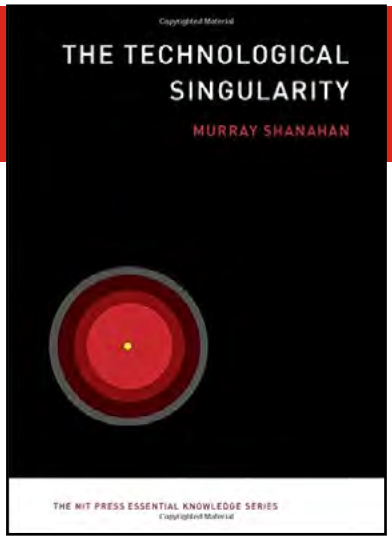

## Libro:
## THE SILENT INTELLIGENCE: THE INTERNET OF THINGS

**Autor:** Daniel Kellmereit y Daniel Obodovski
**Num. Páginas:** 166
**Editorial:** DND Ventures
**Año:** 2013
**Precio:** 9.95 Euros
**Sinopsis:** Kellmereit y Obodovski analizan los retos del Internet de las Cosas. Para ello, tomarán como base un conjunto de entrevistas realizadas con los principales expertos de empresas u organismos como Google, SAP, MIT o Ericsson.




## Libro:
## THE RISE OF THE ROBOTS

**Autor:** Martin Ford
**Num. Páginas:** 352
**Editorial:** Oneworld
**Año:** 2016
**Precio:** 15.00 Euros
**Sinopsis:** Martin Ford analiza como la evolución de la inteligencia artificial está acelerando el uso de los robots y como este uso está impactando en la evolución de la economía mundial.




## Libro:
## THE TECHNOLOGICAL SINGULARITY

**Autor:** Murray Shanahan
**Num. Páginas:** 272
**Editorial:** MIT Press
**Año:** 2015
**Precio:** 16.00 Euros
**Sinopsis:** Shanahan realiza un análisis quirúrgico sobre la delgada línea roja que separa a la tecnología como habilitador para la evolución humana o como principal causante de su destrucción.

# 7.2 Webs recomendadas

**https://turing.ac.uk/**
Sitio web del Instituto Alan Turing, creado conjuntamente en 2015 por las universidades de Oxford, Cambridge, Edinburgh, Warwick y London.

**http://www.datasciencecentral.com/**
Data Science Central es un repositorio de noticias, informes y análisis de profesionales relacionados con el mundo del Big Data.

**https://cyberexchange.uk.net/**
Cyber-Exchange es una organización sin ánimo de lucro británica que promueve la colaboración en materia de ciberseguridad entre el gobierno, la industria y la comunidad universitaria.

**https://www.cert.be/**
Sitio web del Centro de Respuesta a incidentes cibernéticos del gobierno de Bélgica.

**https://www.thehaguesecuritydelta.com/**
Sitio web de The Hague Security Delta, uno de los mayores clúster tecnológicos de Europa en materia de seguridad de la información.

**https://www.encs.eu/**
Sitio web del European Network for CyberSecurity (ENCS), una organización sin ánimo de lucro que aglutina a las principales empresas energéticas de Europa.

# 7.3 Cuentas de Twitter

**@CESG_HMG**

**@cse_cst**

**@turinginst**

**@DataScienceCtrl**

**@tsecrime**

# 8 Eventos

| FECHA | LUGAR | ORGANIZADOR | TÍTULO | URL |
|---|---|---|---|---|
| 6 - 7 Julio | Londres | CIFI | CIFI Europe (The CIFI Security Summit 2016) | http://cifi.network/london2016.html |
| 7 - 8 Julio | Munich | ACPI | 15th European Conference on Cyber Warfare and Security ECCWS | http://www.academic-conferences.org/eccws/eccws2016/eccws16-home.htm |
| 13 julio | Londres | City & Financial Global | 3rd Annual Financial Services Cyber Security Forum | http://www.cityandfinancialconferences.com/events/3rd-annual-financial-services-cyber-security-summit/event-summary-94adef9643cc43be8669c709ce176a11.aspx |
| 16 julio | Sheffield, United Kingdom | SteelCon | SteelCon | https://www.steelcon.info/ |
| 22 - 24 julio | Nueva York | Hope | HOPE 11 | http://www.hope.net/ |
| 27 - 28 julio | Berlin | CONECT GLOBAL LEADERS 2011 | Security of Things World 2016 | http://securityofthingsworld.com/en/ |
| 30 julio - 4 Agosto | Las Vegas, EEUU | Black Hat | Black Hat USA | https://www.blackhat.com/us-16/ |

# Patrocinadores

GOBIERNO DE ESPAÑA — MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

GOBIERNO DE ESPAÑA — MINISTERIO DE DEFENSA

GOBIERNO DE ESPAÑA — MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

GOBIERNO DE ESPAÑA — MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

ACERINOX · AIRBUS GROUP · ATLANTIC COPPER · BBVA

enagas · IBERDROLA · IBM · INDITEX

indra · CaixaBank · MUTUAMADRILEÑA · OHL

RED ELÉCTRICA DE ESPAÑA · renfe · REPSOL

Santander · Telefónica

# Consejo Asesor Empresarial

CAF BANCO DE DESARROLLO DE AMÉRICA LATINA · endesa

IBERIA · Fundación Cajasol

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269