FEBRERO 2016 / Nº 11

CIBER elcano

REAL INSTITUTO elcano ROYAL INSTITUTE

Desarrollado por:

THIBER

INFORME MENSUAL DE CIBERSEGURIDAD

REAL INSTITUTO
elcano
ROYAL INSTITUTE

Copyright y derechos:

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank

Índice

1 COMENTARIO CIBERELCANO
A vueltas con la atribución cibernética

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

A finales de 2015 Ucrania experimentó un ciberataque contra la red eléctrica estatal que dejó sin suministro, durante varias horas, a más de 80.000 hogares en el Oeste del país. Posteriores análisis forenses del incidente, realizados por expertos ucranianos e internacionales, revelaron que los autores del ciberataque no hicieron uso de tecnologías especialmente novedosas ni sofisticadas. Los atacantes emplearon un malware conocido como *BlackEnergy3* – una variante de *BlackEnergy* supuestamente creado por hackers rusos en 2007 – y utilizado en cientos de ciberataques menores contra países de Europa del Este, en especial Polonia. Tal y como constatarían expertos internacionales, los daños causados a la red eléctrica estatal ucraniana fueron reducidos pero evidenciaron la obsolescencia de la misma –lo que paradójicamente permitió una recuperación más temprana al no depender tanto de las nuevas tecnologías - y su imposibilidad para hacer frente a determinados ciberataques.

A mediados del pasado Enero, las autoridades ucranianas alertaban de un ciberataque – haciendo uso de una nueva variante de *BlackEnergy* – contra los sistemas informáticos del aeropuerto de Boryspil que, situado a 30 kilómetros de Kiev, es el más importante de Ucrania y en el que operan el grueso de los vuelos internaciones del país.

Estos últimos ciberataques han provocado que el Gobierno ucraniano haya anunciado una revisión "profunda" de la seguridad de la infraestructura cibernética del país. No obstante, este anuncio resulta paradójico ya que, a principios de 2014, coincidiendo con la crisis política en Ucrania y la escalada bélica sobre la península de Crimea, Ucrania fue objeto de innumerables ciberataques y muchos analistas de defensa plantearon la posibilidad de que Moscú lanzase una ciberoperación como parte integral de una hipotética operación militar híbrida contra Ucrania. La crisis de 2014 puso de manifiesto que el gobierno de Kiev no disponía de ninguna capacidad de respuesta real ante una ciberoperación rusa, por lo que dependía del apoyo que pudiese recibir por parte de alguno de sus aliados.

A pesar del alto nivel de coordinación de los ataques contra los servicios públicos ucranianos, la utilización de malware de origen ruso y los informes internos de los servicios de inteligencia ucranianos que apuntan con el dedo acusador a Moscú, muchos expertos internacionales recuerdan que no es suficiente para atribuir al Kremlin la plena autoría de estos ciberataques. Estas herramientas pueden ser adquiridas en el mercado negro por cualquier banda de cibercriminales u organización estatal para realizar un ataque de falsa bandera. No obstante, en este caso ello parece poco probable.

Sin duda, la determinación de la atribución de un ataque cibernético continúa siendo el mayor escollo con el que se hallan los gobiernos en este ámbito, puesto que hoy en día no es posible, desde el punto de vista tecnológico, determinar con absoluta certeza el autor material de un ataque. Esto requiere un análisis más amplio que añada variables relacionadas con el contexto geopolítico del conflicto al problema de la atribución.

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL

Europa y España: el dilema del panóptico cibernético

AUTOR: Ángel Vallejo. Responsable de Relaciones Institucionales. Socio de Maio Legal.

UN MUNDO VIGILADO

I.- Jeremy Bentham ideó, en 1791 y por encargo de Jorge III, un sistema penitenciario que permitiera un control de la población reclusa a través de un mínimo número de vigilantes, que permanecerían en el interior de una torre central desde la cual podrían observar las celdas establecidas en una construcción circular.

El panóptico partía de un concepto que englobaba una interesante componente de optimización de recursos (pocos vigilantes a cargo de muchos reclusos, en contraposición al sistema clásico), además de una muy relevante consideración psicológica: los vigilantes no podían ser vistos por los reclusos, debido a la configuración física y a las características de los cristales de la unidad central.

"El poder no verificable no deja de ser efectivo por el hecho de no ejercerse en todo momento"

De este modo los internos no podían saber cuándo estaban siendo observados por los vigilantes y cuándo no. La necesaria pulsión era, lógicamente, la de comportarse en todo momento como si estuvieran siendo vigilados. Una unión perfecta de autocensura y heterocensura, maquiavélica en su planteamiento y, al menos en teoría, impecable en su efecto. El poder no verificable no deja de ser efectivo aunque no se ejerza de hecho en todo momento:

"…el efecto principal del panóptico es crear en el interno un estado de conciencia sobre su visibilidad permanente que asegura el funcionamiento automático del sistema. La vigilancia es permanente en sus efectos, incluso si es discontinua en su acción" [1]

II.- Desde los atentados del 11-S Occidente ha vivido en una suerte de estado de alarma en lo relativo al libre ejercicio de los derechos fundamentales que los ciudadanos tienen a la libertad, la seguridad y la privacidad (comunes en lo esencial en todo nuestro entorno cultural y reconocidos en el caso de España en los artículos 17 y 18 de nuestra Constitución).

Los norteamericanos constataron con sorpresa que sus servicios de inteligencia habían sido incapaces de prevenir dichos atentados, pese a que Estados Unidos contaba con una de las maquinarias de espionaje y defensa más potentes del mundo.

[1] Foucault, Michel, en "Surveiller et punir: Naissance de la prison" (Vigilar y Castigar. Nacimiento de la Prisión), París 1975.

Esta dolorosa revelación sirvió de acicate a los gobernantes de la primera potencia para volcarse en acompasar sus capacidades a la dinámica vertiginosa del desarrollo de las Tecnologías de la Información y la Comunicación (TIC) y, sobre todo, a las exigencias estratégicas de un mundo globalizado, donde el dominio de Internet y del ciberespacio se han convertido en un objetivo de primer orden, no sólo para garantizar una seguridad que otrora Occidente daba por descontada, sino para ganar mayores cuotas de poder. En este contexto se hicieron públicas las noticias del ex-agente de la National Segurity Agency americana, (NSA), Edward Snowden.

III.- En esta carrera por dominar el ciberespacio, en un entorno en el que el enemigo a batir es un nuevo tipo de delincuencia que se ha mostrado muy eficaz, el miedo y la complacencia de los propios ciudadanos han sido clave para que muchos gobernantes hayan podido destinar cada vez mayores fondos (aún en años de crisis económica) a sus organismos de inteligencia, ciberespionaje y ciberdefensa, y han proporcionado el marco idóneo para la aprobación de normas cada vez más intrusivas.

El legislador estadounidense había aprobado la Patriot Act *(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)*, normativa modificadora de la FISA *(Foreign Intelligence Surveillance Act)*, que otorgó amplísimas facultades al gobierno y sus agencias para la interceptación de virtualmente cualquier intercambio de información (mediante escuchas telefónicas, captación de comunicaciones analógicas o digitales, etc.), no sólo de sospechosos de espionaje o terrorismo, sino de cualquier ciudadano, nacional o extranjero, y todo ello con poco o nulo control judicial previo[2].

Este fértil ambiente propició una hipertrofia de la NSA, configurada hoy como, probablemente, el agente más tecnológicamente avanzado

[2] Vallejo, Ángel y Rubiales, Julia, en *Hacia una Patriot Act del viejo continente: quo vadis Europa?* Ciberelcano nº 5. Julio de 2015.

del mundo en materia de ciberseguridad, ciberespionaje y ciberdefensa. Su estructura institucional y casi omnipresente interdependencia asimétrica de la industria, de las empresas (públicas y privadas) y de las universidades americanas[3] habría llevado (si damos por buenas las revelaciones de Snowden en junio de 2013 en The Guardian y The Washington Post) a varios gigantes tecnológicos como Apple, Google, Yahoo o Facebook, a colaborar con la NSA facilitando datos protegidos de sus usuarios.

La primera reacción de estas compañías fue negar tales prácticas de colaboración o delación, si bien luego alguna de ellas manifestó haber atendido los requerimientos que consideró legítimos de las autoridades gubernativas, con base en la FISA o en normativa de implementación de la misma. Frente a la corriente colaborativa se colocaron compañías como Lavabit, que mantuvieron la postura (considerada en aquel momento libertaria) de no acceder a las peticiones de las agencias, llegando a abandonar la actividad mercantil con tal de no facilitar el acceso a lo que consideraban el corazón de la confianza de sus clientes y del principio de intimidad y libertad de las comunicaciones.

Sea como fuere, todas estas revelaciones y casos constituyeron el caldo de cultivo idóneo para un cambio de mentalidad posterior, que para sorpresa de muchos, parece comenzar a cuajar actualmente en la cabeza del usuario del ciberespacio en sentido amplio.

LA REACCIÓN EUROPEA

I.- Este nuevo esquema mental, junto con la tozudez de la realidad y la velocidad de desarrollo de las TIC, está llevando a muchos gobiernos y legisladores occidentales a matizar sus posicionamientos estratégicos y legislativos inmediatamente posteriores al 11-S y a otros ataques y ciberincidentes más recientes. La reacción estadounidense ante el cambio de paradigma que el 11-S supuso en todo el mundo, ha tenido su eco también en Europa. El nuevo marco internacional y la actividad de lobby difuso de multitud de comunicadores de gran relevancia en el ciberespacio han propiciado cambios regulatorios de calado en el viejo continente.

"Este nuevo esquema mental, junto con la tozudez de la realidad y la velocidad de desarrollo de las TIC, está llevando a muchos gobiernos y legisladores occidentales a matizar sus posicionamientos estratégicos y legislativos inmediatamente posteriores al 11S"

Estos cambios se han implementado unas veces en línea con las primeras reacciones sobreaseguradoras del gigante americano (hoy atemperadas por la aprobación en el Senado en junio de 2015 de la USA Freedom Act, que

[3] Fojón, Enrique, Colom, Guillem y Hernández, Adolfo, en *La Agencia de Seguridad Nacional (NSA), el espionaje y la colaboración público-privada en EEUU.* Real Instituto Elcano. ARI 41/2013. 11 de noviembre de 2013.

impone límites a muchos de los programas de recopilación de información de la NSA) y otras veces siguiendo el espíritu de protección y amparo que tradicionalmente ha primado en Europa con relación a los derechos fundamentales de sus ciudadanos.

II.- Reino Unido y Francia se han convertido en los representantes de la corriente más transgresora (por intrusiva) que existe hoy en Europa ante la constante y creciente amenaza del terrorismo internacional y la ciberdelincuencia. En el primer caso, con la aprobación en junio de 2015 de una ley que limita enormemente la responsabilidad de los servicios de inteligencia, la policía y del Centro Gubernamental de Comunicaciones británicos (GCHQ - *Government Communications Headquarters*), en relación con las acciones de hacking e interceptación de comunicaciones que realicen frente a cualquier persona sin previa autorización judicial. En el segundo caso, con la aprobación por la Asamblea Nacional Francesa, tras el atentado de Charlie Hebdo, de una ley de seguridad y antiterrorismo que otorga a los servicios secretos franceses mayores medios técnicos y una amplia cobertura en la interceptación de comunicaciones, el acceso a redes y bases de datos, así como para obligar a los operadores de telecomunicaciones a colaborar en estas labores, también sin control judicial previo.

EL CAMINO ESPAÑOL

I.- El primer movimiento:

España inició la revisión de su legislación penal y procesal en lo que respecta a los poderes de investigación basados en las TIC siguiendo la senda más intrusiva de la primera reacción estadounidense tras el 11-S. El afán reformista, en su vertiente más orwelliana, partía de un proyecto que preveía la intervención y conocimiento del contenido de las comunicaciones telefónicas de los procesados, sin necesidad de una previa resolución judicial debidamente motivada que autorizase estas medidas. En concreto, el texto del Anteproyecto de la vigente Ley de Enjuiciamiento Criminal (LECR) permitía la captación de comunicaciones y datos, ya fuera a través de "pinchazos" o mediante el uso de "troyanos" por las fuerzas de seguridad, sin necesidad de contar con autorización judicial previa.

La tendencia americanizante ha tenido, sin embargo, serios obstáculos en Europa y desde luego en España. La sentencia de octubre de 2015 del Tribunal de Justicia de la Unión Europea, en el caso Maximillian Schrems/Data Protection Commissioner, volvió a cambiar el rumbo europeo en tema de seguridad y protección de datos. Esta resolución judicial declaró inválida la Decisión de la Comisión de 26 de julio de 2000 (el Acuerdo *Safe Harbour*), sobre transferencia de datos personales de ciudadanos de la UE a Estados Unidos. La sentencia obligaba a plantear a Irlanda (Estado Miembro involucrado en el procedimiento), y por extensión al resto

de miembros de la Unión Europea, la necesidad de suspender la transferencia automática de datos de los usuarios europeos de Facebook a Estados Unidos por no acreditarse de manera suficiente que la compañía norteamericana pudiera ofrecer un *"nivel de protección adecuado de los datos personales"*.

El caso *Safe Harbour* (y, antes de él, una fuerte y continua oposición de buena parte de la comunidad jurídica más especializada en el derecho de las TIC y su relación con los poderes intrusivos de investigación del gobierno español y sus agencias) ha llevado a que España, no sin ciertos conatos de seguir los más recientes ejemplos inglés o francés, haya optado finalmente por implementar la normativa más fiel al citado espíritu europeo, esto es, el que construye sus principios sobre un elevado marco de protección de los derechos fundamentales de sus ciudadanos.

"Todos ellos vienen obligados por la LECR a colaborar con los Tribunales, el Ministerio Fiscal y la Policía Judicial, y a guardar secreto respecto de las actuaciones que realicen en el marco de las investigaciones judiciales en las que participen"

II.- El planteamiento del panóptico cibernético gubernativo:

a.- La vigente LECR (en su Libro II, Título VIII, Capítulos IV a X, artículos 588 bis a 588 octies) exige finalmente, y en todo caso, la autorización previa y el control posterior de los tribunales para que, ya sea de oficio o a petición del Ministerio Fiscal o la Policía Judicial, puedan llevarse a cabo medidas consistentes en: la interceptación de comunicaciones telefónicas y/o telemáticas; la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen; el registro de dispositivos de almacenamiento masivo de información; o el registro remoto sobre equipos informáticos.

Según su artículo 588 *bis* a), en la solicitud, adopción y ejecución de cualquiera de estas medidas habrá de primar en todo caso un escrupuloso respeto a los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

Muchas de las medidas de investigación antes referidas no pueden llevarse a cabo sin la colaboración de los prestadores de servicios de telecomunicaciones, de acceso a la red de telecomunicaciones o de servicios de la sociedad de la información, así como de toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual.

Todos ellos vienen obligados por la LECR a colaborar con los Tribunales, el Ministerio Fiscal y la Policía Judicial, y a guardar secreto respecto de las actuaciones que realicen en el marco de las investigaciones judiciales en las que participen.

Esa obligación de asistir y colaborar va intrínsecamente unida a la de guardar secreto sobre dicha obligación y las actuaciones realizadas en cumplimiento de la misma,

pudiendo incurrir la persona o entidad que no colabore en un delito de desobediencia (delito castigado, según el artículo 556 del Código Penal, con una pena máxima de un año o multa de seis a dieciocho meses).

Pero esa obligación de asistencia y colaboración por parte de los operadores antes referidos está también sometida a control judicial. La Policía Judicial debe poner a disposición del Juez, con la periodicidad que éste determine, la transcripción de los pasajes que considere de interés y las grabaciones integras realizadas. La duración máxima que la LECR establece para la medida de injerencia es de tres meses, aunque permite prórrogas por períodos sucesivos de igual duración, hasta un plazo máximo de dieciocho meses.

b.- Los siguientes artículos de la LECR contemplan también sendos deberes de colaboración y secreto: 588 *ter* e), para el caso de la interceptación de las comunicaciones telefónicas y telemáticas; 588 *ter* j), respecto a la incorporación al proceso de datos electrónicos de tráfico o asociados; 588 *ter* k), para la identificación de usuarios, terminales y dispositivos de conectividad mediante números IP; 588 *ter* m), para la identificación de titulares o terminales o dispositivos de conectividad; 588 *quinquies* b), apartados 3 y 4, para la utilización de dispositivos o medios técnicos de seguimiento y localización; 588 *sexies* c), apartados 4 y 5, para el registro de dispositivos de almacenamiento masivo de información; y 588 *septies* a), para el registro remoto de equipos informáticos.

De entre estos preceptos, mención especial merecen el artículo 588 *ter* m), el 588 *quinquies* b), apartado 4, y el 588 *sexies* c), apartados 4 y 5. En todos ellos se contemplan supuestos de urgencia en los que, en unos casos *"el Ministerio Fiscal o la Policía Judicial"*, y en otros *"las autoridades o agentes encargados de la*

investigación", pueden dirigirse directamente a los operadores antes referidos para requerirles información y/o la realización de ciertas actuaciones. Aquéllos estarán obligados a prestar su colaboración y a guardar secreto sobre ésta, so pena de incurrir en un delito de desobediencia. Pero en todos estos casos existe un control judicial posterior sobre las medidas de investigación tomadas y/o sobre la colaboración requerida.

III.- El abrazo a los sistemas garantistas frente a la hipervigilancia en la situación actual

a.- Con la actual LECR los ciudadanos españoles pueden hoy estar algo más tranquilos. La norma en su vigente redacción no permite la interceptación de comunicaciones, el uso de software intrusivo por la Policía Judicial y/o la entrada en sistemas y bases de datos privados, sin que previamente medie una resolución motivada del Juez competente que así lo autorice. En ella deben de estar siempre claramente especificados todos los requisitos (objeto, extensión, forma, duración, etc.) de cada concreta medida de investigación acordada.

"Se ha regulado también (ya era urgente e imprescindible) la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación"

Se ha regulado también (ya era urgente e imprescindible) la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación. Y se establece que su actuación requerirá una autorización judicial especial para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación.

Es decir, se generaliza y asienta la intervención judicial frente a los sistemas de decisión gubernativos. Las únicas excepciones que a día de hoy contempla la norma a la exigencia de dicha autorización judicial previa son los supuestos antes referidos (artículos 588 *ter* m, 588 *quinquies* b, apartado 4, y 588 *sexies* c, apartados 4 y 5), aunque sí existe la necesidad de contar con una ratificación y/o control judicial posterior, que de no darse invalidaría la medida de investigación/colaboración ejecutada en virtud de tales preceptos.

Algo a tener siempre en cuenta es que, sin llegar el asentimiento ciudadano a la idea de una sociedad remedo como la de Matrix, se constata que la mayoría de los occidentales parece haber interiorizado que más seguridad comporta necesariamente cierta transigencia en el respeto a los derechos fundamentales a la libertad y la privacidad.

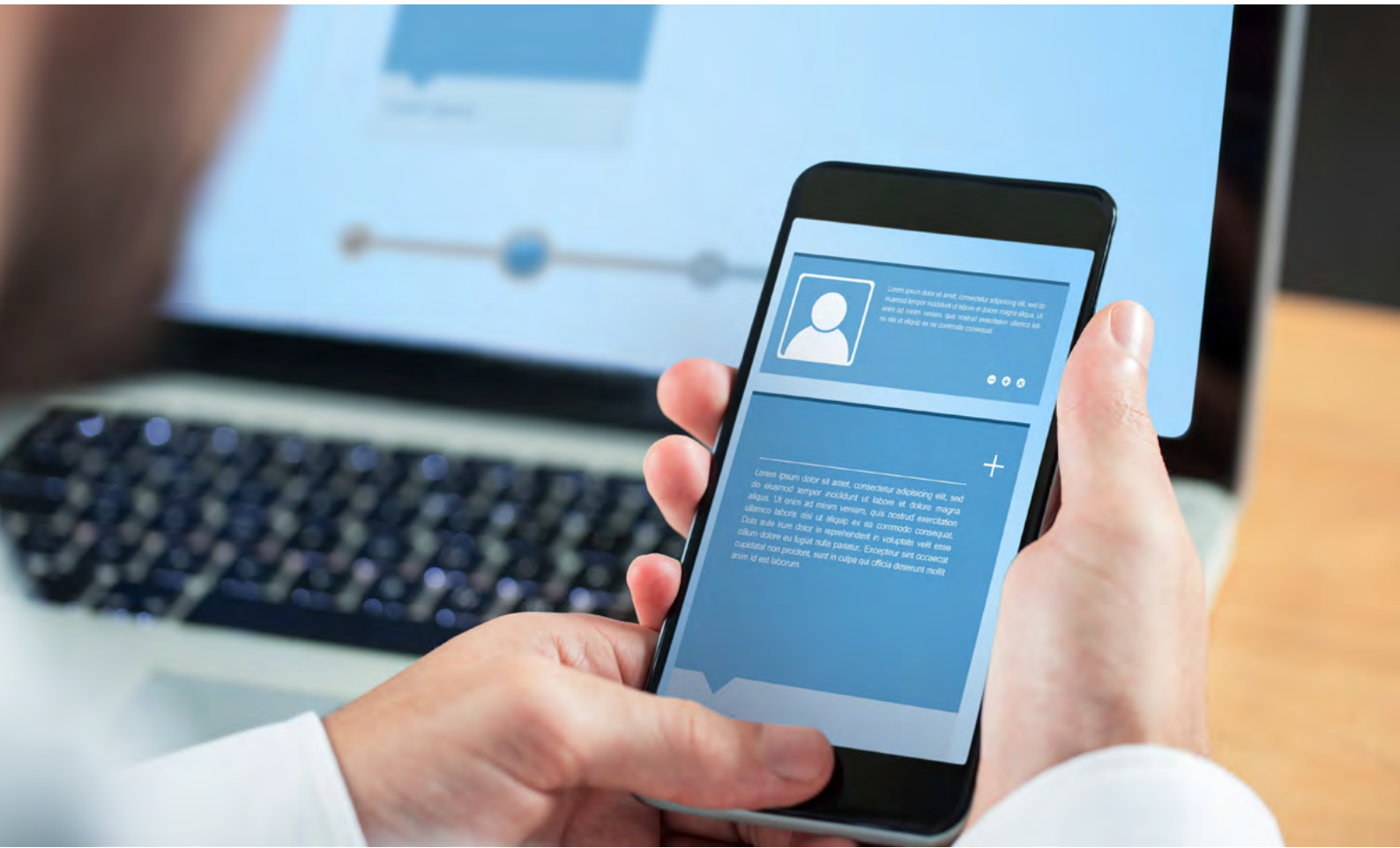
Los hábitos normales del usuario medio del ciberespacio revelan que no pocas veces se asumen alegremente los riesgos asociados al hecho de que nuestros datos más personales queden fuera de nuestro exclusivo control. Nadie lee detenidamente las "condiciones del servicio" antes de consentir la instalación de cualquier programa informático en los ordenadores que vertebran la vida actual, ni cuando se actualiza el Smartphone. Menos aún se observa la saludable práctica de no aceptar tales condiciones cuando advertimos en ellas algo con lo que no estamos de acuerdo.

b.- Es cierto que el creciente clima de desconfianza generado por el caso Snowden, o las revelaciones de Assange o Appelbaum y los ciberincidentes provocados por organizaciones criminales, y aún estatales, han contribuido a que muchos usuarios sean cada vez más conscientes de los riesgos asociados a la navegación por el ciberespacio.

Pero, paradójicamente, el ciudadano consiente una y otra vez potenciales vulneraciones de su privacidad a cambio de objetivos menos comprensibles que el lograr una mayor seguridad. Muchas veces se opta por la comodidad e inmediatez en un mundo que se mueve a velocidad de vértigo, en detrimento del cuidado, del más elemental sentido común y de la salvaguarda de nuestros derechos fundamentales.

Los usuarios demandan cada vez con mayor frecuencia de los operadores de Internet, y de todas las compañías privadas, organismos relacionados de una u otra forma con el ciberespacio, y por supuesto de los gobernantes, la garantía de unos mínimos estándares de seguridad y de protección de su privacidad. Como paradigma encontramos el auge de las compañías que proveen servicios de correo cifrado, como ProtonMail y su lema *"We're building an internet that protects privacy, starting with email"*, compañías que (todo hay que decirlo) afrontan diariamente el hostigamiento de gobiernos y agencias de todo el mundo.

Sin embargo, no debe olvidar el ciudadano que exigir una mayor seguridad y protección, siendo irrenunciable, de nada sirve si no va acompañada primero por una auto exigencia propia de cumplir con unos mínimos de seguridad y de protección. De no exigirse cada ciudadano el cumplir dichos mínimos, poco efecto tendrá la exigencia a las autoridades gubernativas para que se involucren en una mayor protección hacia nuestros



datos, nuestra intimidad y nuestra libertad en el ciberespacio.

c.- En ese ecosistema encontramos lo que parece ser el contradictorio signo de los tiempos y, en opinión de muchos, la grandeza de la resistencia al poder como motor de la evolución social y jurídica, de la negación de una sociedad vigilada y de un mundo feliz presidido por una torre central de observación.

La sociedad, o buena parte de ella, está dispuesta en ocasiones a ceder o renunciar a sus derechos de intimidad, seguridad y libertad en el ciberespacio siempre que esa cesión o renuncia sean decididas voluntariamente en cada caso por el interesado, y nunca impuestas por los actores gubernativos.

Y ahí se inserta la novísima regulación de los procesos de vigilancia, monitorización y control de las comunicaciones y los sistemas tecnológicos que rige desde hace pocas semanas en España. Nuestra LECR, en su literalidad, y ahí reside buena parte de su acierto, parte de reconocer que la tecnología ha venido avanzando a mucha más velocidad que la legislación, pero también declara que la actualización normativa no puede ir en detrimento de las garantías procesales.

La norma española de la que hablamos se construye sobre el *"fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica"*. Y comienza el apartado IV de su preámbulo con el reconocimiento expreso y literal de que *"la Ley de Enjuiciamiento Criminal no ha podido sustraerse al paso del tiempo. Renovadas formas de delincuencia ligadas al uso de las nuevas tecnologías han puesto de manifiesto la insuficiencia de un cuadro normativo concebido para tiempos bien distintos".*

Y sigue exponiendo que *"los flujos de información generados por los sistemas de comunicación telemática advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a tercero"*.

En términos generales, el usuario del ciberespacio en España no ha de sentirse como el interno en la prisión de Bentham. El asentamiento de la opción del control judicial en detrimento de la corriente pro-gubernativa, que sin duda hubiera supuesto una cierta instauración del citado panóptico cibernético es ya, en definitiva, un hecho incontestable en nuestra legislación. Esto no evitará puntuales desviaciones de poder y concretos excesos gubernativos en las actividades de vigilancia, interceptación de comunicaciones de base tecnológica y control de los flujos de información, pero sí ha de evitar que tales excesos adquieran carta de naturaleza, como ha ocurrido hasta hace no tanto en países de nuestro entorno occidental.

3 Entrevista a Juan Cobo.
Chief Information Security Officer (CISO) de Ferrovial.

1. Como responsable de seguridad de la información de Ferrovial, ¿podría indicarnos cuáles son las principales competencias dentro de su área? ¿Cuál es su rol en la implementación de la estrategia corporativa? ¿ha visto un cambio en sus competencias en los últimos años?

El departamento de Seguridad de la Información está integrado dentro de la Dirección General de Sistemas de Información e Innovación. Se concibe como una función corporativa centralizada que cubre de forma integral el gobierno, la gestión y la operación de la Seguridad. Así pues, se cubren aspectos tales como el análisis y la gestión de riesgos tecnológicos, la continuidad de negocio, la seguridad en el ciclo de vida de sistemas y servicios, el awareness de seguridad, el IT compliance, la protección de arquitecturas y perímetros, la gestión de la identidad digital, el control de los accesos, la cibervigilancia, etc. Si bien la responsabilidad sobre la seguridad física de los activos patrimoniales corporativos corresponde a otra Dirección General, existe un instrumento de comunicación y coordinación vertebrado a través del Comité de Seguridad, en el que ambas Direcciones están representadas.

Ferrovial, como empresa ligada a la gestión de infraestructuras de transporte, a la gestión de servicios a ciudades y a la construcción, ha experimentado paulatinamente un fuerte proceso de digitalización. Debido a esta exposición digital, como no puede ser de otra forma, nuestros negocios son más vulnerables a los riesgos

tecnológicos. Este proceso ha provocado un nivel creciente de concienciación y sensibilización por parte de la Dirección. El concepto de seguridad ha calado corporativamente, ya no se pude vivir de espaldas a él.

Por extensión, la función de seguridad de la información ha experimentado un aumento paulatino de competencias y responsabilidades, dando lugar a un modelo corporativo de seguridad con clara vocación de orientación a servicio. En este viaje, contamos con dos partners principales: HP y Telefónica. Así pues, la operación de la seguridad se encuentra externalizada y la gestión permanece y se asume internamente a través del equipo que integra el Departamento.

Adicionalmente, Ferrovial está inmersa en un proceso de globalización del modelo de seguridad corporativo, exportando dicho modelo

a todas las regiones internacionales que cuentan con despliegues tecnológicos locales, evitando el desalineamiento inherente a la gestión local de IT. Es por ello que se ha puesto en marcha un nuevo modelo de reporting, con los roles de local CISO reportando al CISO global.

En cuanto al compliance, siendo ésta una de las dimensiones cubiertas por nuestras competencias, el ámbito de responsabilidad abarca normativas tales como PCI-DSS, LOPD/ Privacidad, SCIIF, marcos de control interno y todas aquellas regulaciones con incidencia en IT o en la seguridad de los activos de información. Nuestra coordinación y colaboración con áreas y funciones externas a Sistemas de Información se articula a través del Comité de Seguridad la Información.

2. ¿Cuáles son las principales amenazas y retos de seguridad a las que se encuentra expuesta una multinacional que opera infraestructuras? ¿se dispone de las herramientas, servicios y el talento necesario a nivel nacional para afrontar dichos retos?

Las ciberamenazas que preocupan a nivel corporativo son, por un lado, todas aquellas que puedan afectar a las infraestructuras operadas y, por otro, las relativas a la pérdida de propiedad intelectual o a la exposición de activos digitales sensibles.

Desde el punto de vista tecnológico, la movilidad (que nos aporta agilidad y flexibilidad), el *Cloud* y el *Big Data*, al ser claras apuestas de la estrategia IT, han abierto nuevos escenarios de

riesgo para los cuales el mercado de la seguridad y las soluciones actualmente disponibles deben seguir madurando. Estos nuevos escenarios constituyen una de nuestras prioridades.

En cuanto a la oferta de servicios y productos en el mercado para cubrir las necesidades expuestas, desde el punto de vista organizativo, tecnológico, procedimental y jurídico, se pueden cubrir parcialmente con empresas nacionales, si bien no podemos olvidar que Ferrovial es una compañía global que requiere de partners tecnológicos globales (nacionales e internacionales) que nos acompañen en todos aquellos países en los que estamos presentes.

Por cierto, no quiero pasar por alto que el talento nacional en materia de seguridad siempre ha gozado de muy buena salud.

3. Como gestor de grandes infraestructuras como aeropuertos y autopistas que potencialmente, pueden ser identificadas como infraestructuras críticas, ¿este tipo de activos afrontan nuevos vectores de ataque o son los mismos que se identificaban en el ámbito TIC tradicional?

En España no operamos infraestructuras catalogadas, a día de hoy, como críticas. En Reino Unido, obviamente, sí.

La gestión de las grandes infraestructuras, como los aeropuertos de Heathrow, Glasgow, Aberdeen y Southampton, supone un reto, una responsabilidad, un desafío y mucho trabajo.

Efectivamente, este tipo de activos afrontan nuevos vectores de ataque en la medida en que las ciberamenazas evolucionan de forma vertiginosa y el escenario es diferente, pero no debemos infravalorar los vectores que ya se identificaban en el ámbito TIC tradicional, muchas veces también de aplicación.

En muchas ocasiones, los ciberataques exitosos no explotan vulnerabilidades novedosas, sino vulnerabilidades bien conocidas, incluso antiguas, que no han sido convenientemente gestionadas.

" La gestión de las grandes infraestructuras, como los aeropuertos de Heathrow, Glasgow, Aberdeen y Southampton, supone un reto, una responsabilidad, un desafío y mucho trabajo."

4. La competencia de protección y gestión de la seguridad en las infraestructuras críticas, si bien está regulada, ¿cree que en grandes compañías debería ser competencia del CISO o bien un rol independiente con coordinación funcional con éste?

En mi opinión, no debe ser responsabilidad exclusiva del CISO, pero el CISO sí debe jugar un papel protagonista en la protección. Eso sí, al margen de lo estrictamente regulado, no creo que existan fórmulas magistrales para organizar las responsabilidades en materia de seguridad. Cada compañía, cada Negocio debe contextualizar y adaptar su organización a sus propias necesidades.

En nuestro caso, de cara a la protección, se apuesta por la coordinación entre las distintas áreas (dentro y fuera de IT) con responsabilidad en la materia. En el caso concreto de aspectos relativos a Ciberseguridad, como comenté

anteriormente, y conforme al modelo global desplegado, existe un responsable local (Local CISO) para dichas infraestructuras, reportando funcionalmente al Global CISO, responsable del despliegue local del catálogo de controles asociados a dicho modelo y de aplicación en todas las líneas de negocio.

5. Bajo la óptica de una gran multinacional del sector construcción y servicios, ¿qué medidas de control o de coordinación echa en falta por parte entre las compañías del sector con el objetivo de mejorar la respuesta ante ciberincidentes? ¿se comparte información?

Necesitamos más coordinación y comunicación, al menos desde un punto de vista formal. Cuando se habla de colaboración y de compartición en nuestro sector, suelen ser actuaciones bilaterales, realizadas casi siempre en el ámbito de la relación cordial con otros colegas del sector. Por lo tanto, sería necesario una mayor formalización en ese aspecto.

De forma general, la compartición de información tiene todavía un largo recorrido. En nuestro caso, a pesar de no ser operadores de infraestructuras críticas, hemos firmado un acuerdo con CNPIC e INCIBE para, entre otras cosas, mejorar la compartición de información sobre ciberamenazas e incidentes. En materia de comunicación, coordinación y colaboración, en mi opinión, la Administración debe jugar un papel protagonista como habilitador en esta temática, liderando de forma proactiva estas iniciativas.

6. ¿Cuál cree que será el panorama de ciberamenazas futuras ante las que deberá estar preparada una entidad que gestiona y opera grandes infraestructuras?

Claramente, nos enfrentamos a un escenario creciente de amenazas, en número y en complejidad. Tenemos mucho trabajo por delante, también de la mano de las tendencias de mercado actuales aplicables a nuestros negocios, tales como Smart Cities, Internet de las Cosas, Digitalización, Movilidad o Big Data; y sin olvidar tampoco los nuevos hábitos, como el Shadow /T.

Todo ello bajo la misma premisa: la creciente interconexión. Si estás conectado, eres vulnerable.

7. Desde el punto de vista de la estrategia de gestión de riesgos de seguridad corporativos, ¿considera que las estrategias de transferencia de riesgos a través de pólizas de seguro son una realidad viable? ¿está maduro este sector en España?

No sólo creo que son iniciativas interesantes sino que en el medio plazo serán fundamentales.

Otra cosa es el nivel actual de madurez. Por nuestra parte, hemos analizado la oferta actual de mercado, pero sigue habiendo gaps importantes entre las coberturas y nuestras necesidades.

8. Si tuviese que exhortar al legislador o al Ejecutivo para mejorar la resiliencia de las grandes compañías ante ciberataques, ¿qué solicitaría como CISO?

Una implicación creciente de la Administración en la gestión de la ciberseguridad. Reconociendo que estamos en el buen camino (ahí está la Estrategia de Ciberseguridad Nacional, el CNPIC, el INCIBE, el CCN, las Fuerzas y Cuerpos de Seguridad del Estado, las diferentes regulaciones ...) sigue llamándome la atención cómo la involucración estatal en el mantenimiento de la seguridad física, tradicional, obvia para todos, tiene todavía un largo recorrido en el terreno digital.

Así pues, ambos mundos, el físico y el digital, y el papel de la Administración como garante en primera instancia de la protección de ambos, deberían quedar armonizados paulatinamente. Pediría también que en dicha armonización se tuviese en cuenta la voz de la empresa privada y de industria, a fin de que no se regule de espaldas a nuestras necesidades.

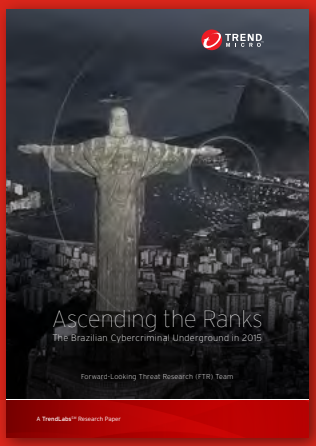
Como CISO, estoy totalmente convencido de que así debería ser.

"sigue llamándome la atención cómo la involucración estatal en el mantenimiento de la seguridad física, tradicional, obvia para todos, tiene todavía un largo recorrido en el terreno digital."

4 Informes y análisis sobre ciberseguridad publicados en enero de 2016

Guía de Seguridad ICC para los negocios (Camaras de Comercio Internacional)

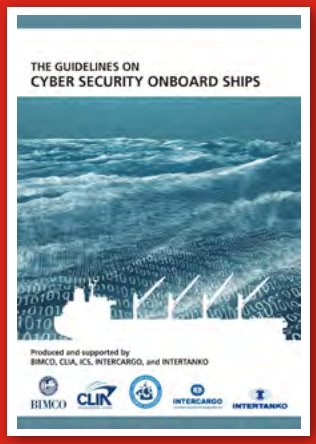
The Brazilian Cybercriminal Underground in 2015 (Trend Micro)



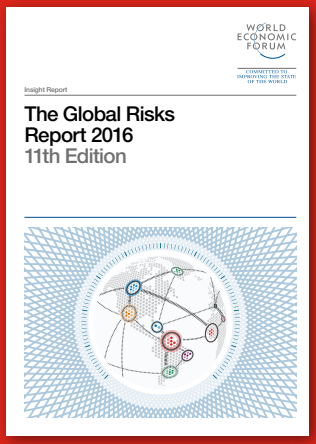
ENISA Threat Landscape 2015

Big Data Threat Landscape (ENISA)

The Guidelines on cybersecurity onboardhips (INTERCARGO)

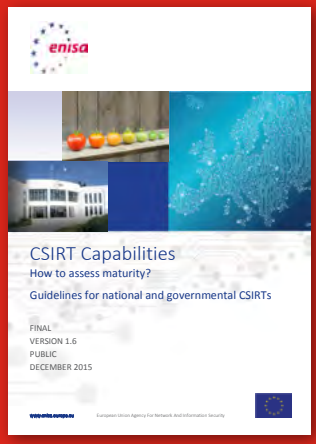


The Global Risks Report 2016 (World Economic Forum)



RiskMap Report (Control Risks)

CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs (ENISA)



5 HERRAMIENTAS DEL ANALISTA: OpenSoc

El *OpenSOC* Project es un proyecto de código abierto colaborativo dedicado a ofrecer una herramienta de análisis de seguridad avanzada extensible y escalable basado en Apache Hadoop, diseñado para trabar en escala. El proyecto OpenSOC tiene los siguientes objetivos:

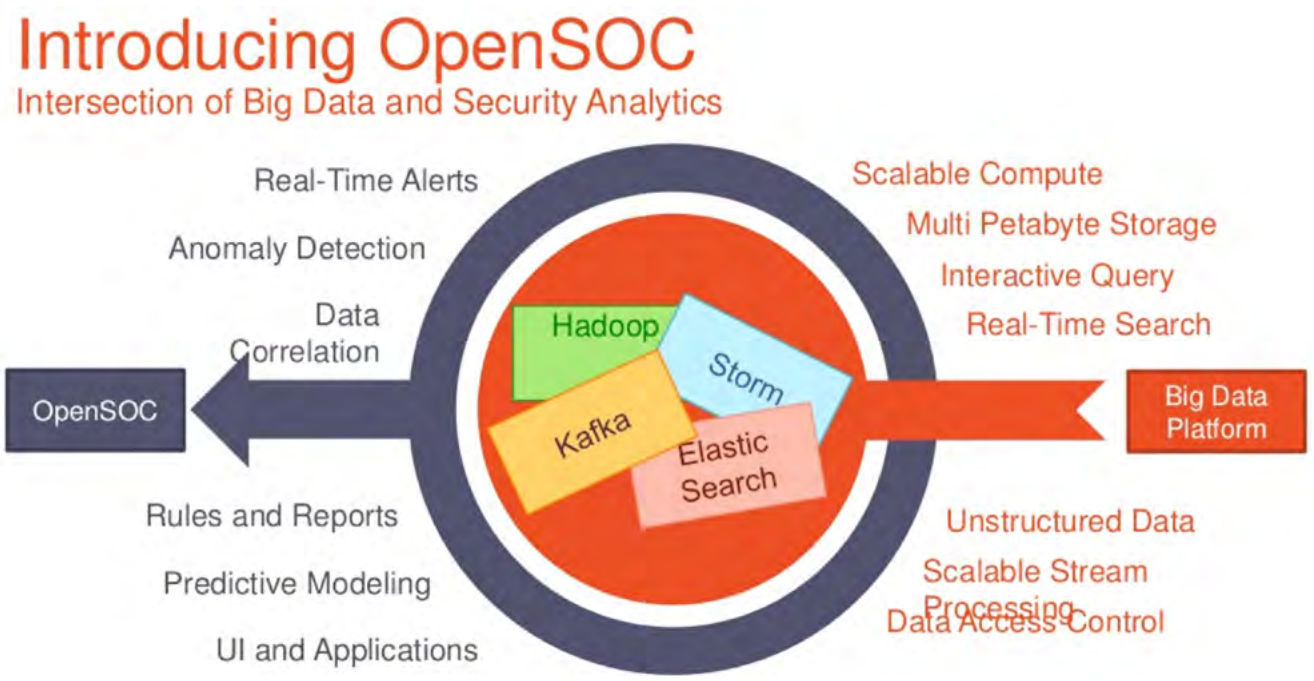
- Para proporcionar una comunidad de código abierto de colaboración para el desarrollo de una herramienta de análisis de seguridad avanzada extensible y escalable

- Fomentar la comunicación abierta para funciones adicionales y la identificación de las deficiencias de una herramienta estable y funcionalmente útil

- Para identificar las mejoras de las características clave de los esfuerzos para impulsar la tecnología de todo análisis de seguridad eficientes

OpenSOC es un marco de análisis de seguridad de grandes volúmenes de datos diseñado para consumir y controlar los datos de tráfico de red y de salida de un centro de procesamiento de datos. OpenSOC es extensible y está diseñado para trabajar a una escala masiva.

OpenSOC proporciona capacidades para la agregación de logs, indexado completo de paquetes de datos, almacenamiento, análisis avanzado de comportamiento y enriquecimiento de datos, mientras que la aplicación de la información más actualizada la información sobre amenazas de seguridad dentro de una sola plataforma.



OpenSOC puede ser dividido en cuatro áreas:

- Un mecanismo para capturar, almacenar y normalizar cualquier tipo de datos de seguridad a velocidades extremadamente altas. Debido a que constantemente se está generando telemetría de seguridad, se requiere un método para la ingesta de datos a altas velocidades y pasándolos por diversas unidades de procesamiento para el cálculo y análisis avanzados.

- Procesamiento en tiempo real y la aplicación de enriquecimiento tales como inteligencia de amenazas, geolocalización y la información de DNS. La aplicación inmediata de esta información proporciona perspectiva sobre el contexto, así como datos sobre el quién y el dónde, puntos críticos para una investigación de seguridad de la información.

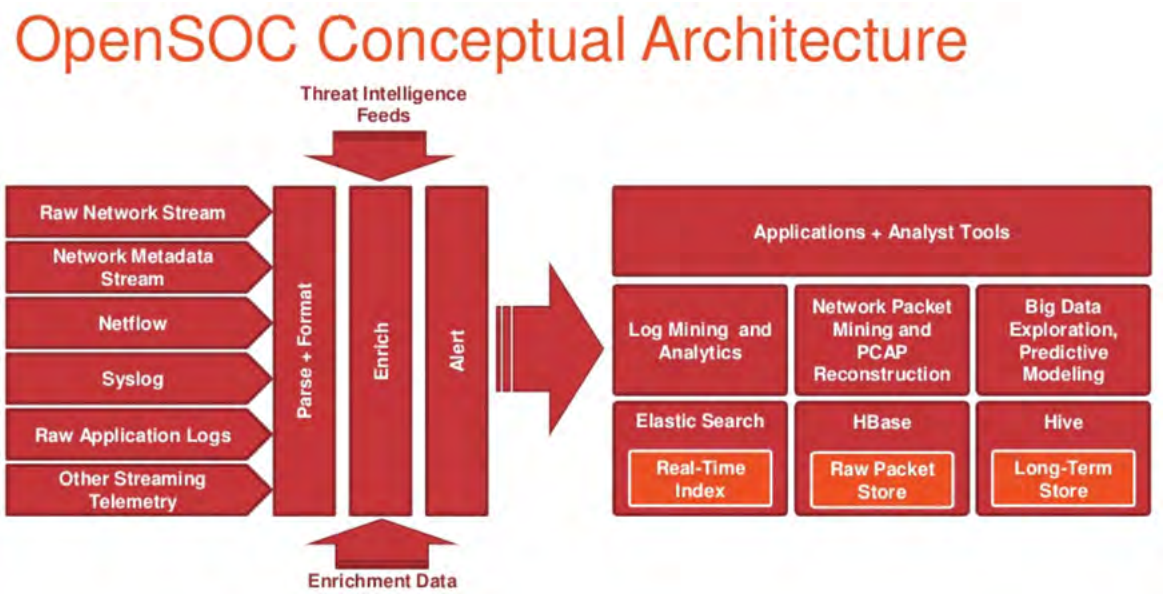
- Almacenamiento eficiente de información, basado en cómo se utilizará dicha información:

    - Logs y telemetría se almacenan de tal manera que pueden ser extraídos y analizados con facilidad para dar visibilidad concisa y eficiente sobre ciberamenazas.

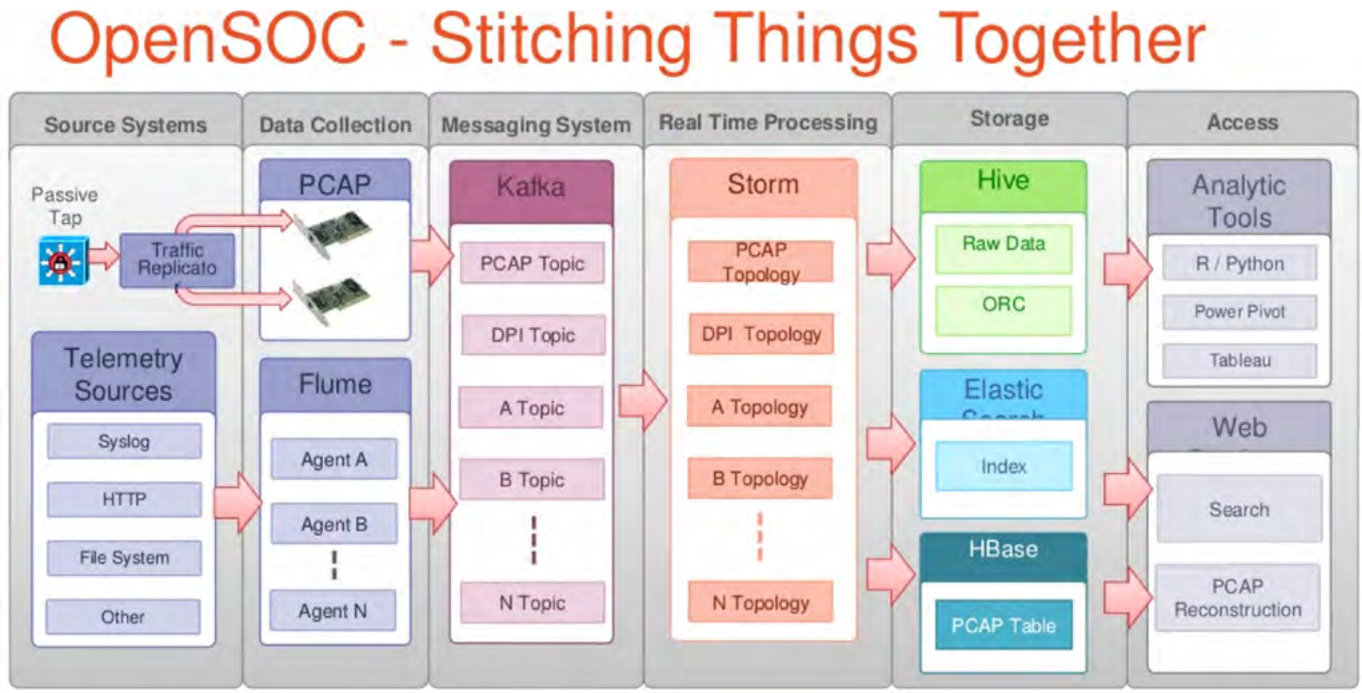
    - Capacidad de extraer y reconstruir paquetes completos ayuda a un analista a responder preguntas tales como quién era el verdadero atacante, qué datos se filtraron, y donde fueron enviados.

    - El almacenamiento a largo plazo no sólo aumenta la visibilidad en el tiempo, sino que también permite el análisis avanzado, tales como técnicas de aprendizaje automático que se utilizarán para crear modelos de información. Los datos de entrada pueden ser contrastados contra estos modelos para la detección de anomalías avanzada.

- Una interfaz que da un investigador de seguridad una vista centralizada de los datos y las alertas de un sistema. La interfaz del OpenSOC presenta resúmenes de alertas con la información sobre amenazas y los datos de enriquecimiento específico de dicho alerta en una sola página. Por otra parte, también ofrece capacidades avanzadas de búsqueda y herramientas de extracción de paquetes completos.



El Big data es un paso natural para potenciar el análisis de eventos de seguridad. OpenSOC integra una serie de elementos del ecosistema Hadoop para proporcionar una plataforma escalable para el análisis de seguridad, incorporando dicha funcionalidad como la captura de paquetes completa, procesamiento de flujo, el procesamiento por lotes, búsqueda en tiempo real, y la agregación de feeds.



6 Análisis de los Ciberataques del mes de enero de 2015

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

CIBERCRIMEN

A principios de enero, los investigadores de IBM X-Force detectaron al un grupo de cibercriminales a los que se les atribuye la autoría del *troyano bancario Rovnix*, estando éste implicado en una agresiva campaña contra catorce grandes bancos japoneses.

La campaña, que ha estado activa desde mediados de diciembre del año pasado, infectaba a los usuarios con un troyano mediante un ataque de phising, ocultándolo en un programa de descarga en un correo electrónico haciéndose pasar por una empresa de transporte internacional en el cual ofrecían la visualización de una factura.

Ilustracion: Campaña de Rovnix focalizada en entidades financieras japonesas

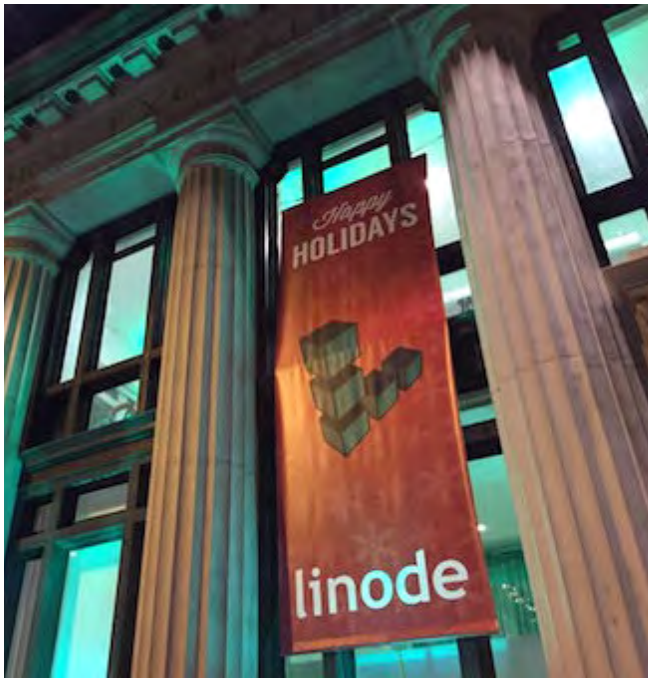
Time Warner Cable (TWC), el segundo mayor proveedor de cable de Estados Unidos, tras una investigación realizada por el FBI, *reconoció el robo de las credenciales de inicio de sesión de más de 320.000 clientes.*

De acuerdo con TWC, la información filtrada incluye direcciones de correo electrónico de los clientes y las contraseñas de dichas cuentas - información utilizada para iniciar sesión en el portal de servicio al cliente de TWC- . No hay ninguna indicación adicional relativa a las tarjetas de pago u otra información personal se podría haber visto potencialmente comprometidos, pero en la comunicación que está realizando TWC a los clientes afectados, recomiendan verificar los movimientos bancarios en los próximos meses.

Según las últimas informaciones, puede tratarse de una campaña de phising dirigida en lugar de un robo de información.

Por otra parte, tras hacer frente con un ataque DDoS de larga duración hace algunos meses, *Linode ha reportado una fuga de información de credenciales* tras haber verificado la existencia de esta información en un "servidor externo" a la compañía. Como medida mitigatoria, han ejecutado un restablecimiento de contraseña de todo el sistema de cuentas de clientes.

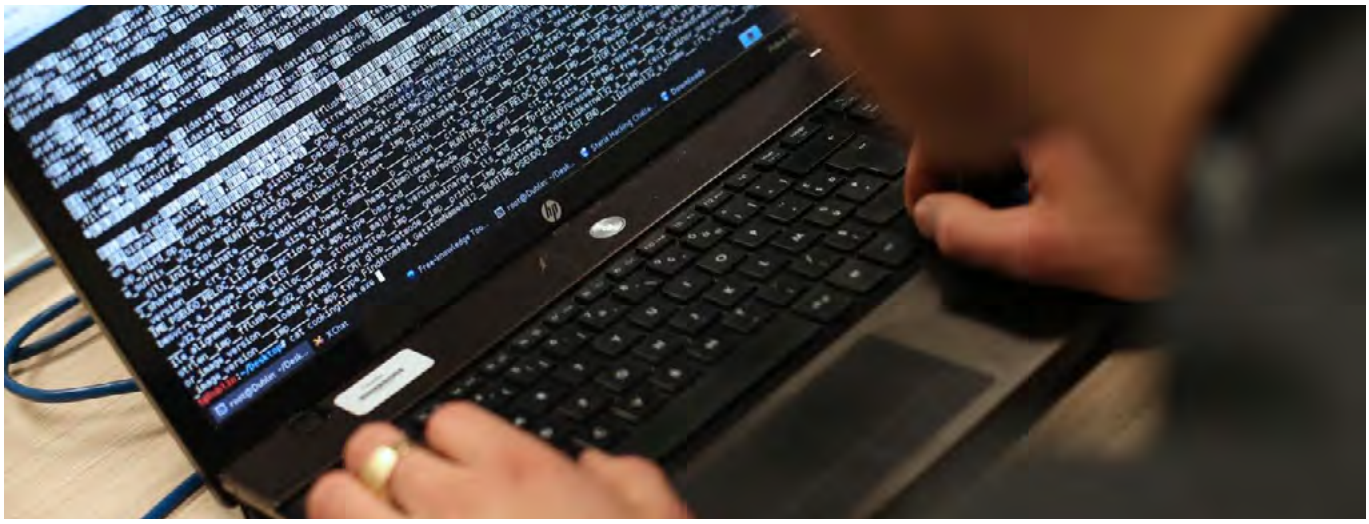
El aviso publicado por la propia compañía, dice que la fuga "implica credenciales de usuario podrían haber sido leídos de nuestra base de datos, ya sea en línea o fuera de, en algún momento."



A mediados de enero, *un hacker ruso responsable del desarrollo de un malware conocido como "W0rm"*, mediante un ataque de fuerza bruta sobre credenciales débiles – usando como usuario press@citrix.com contraseña Citrix123 – pudo conseguir acceso en el sistema de gestión de contenidos de Citrix, accediendo la información personal de un gran número de clientes.

El atacante (W0rm) publicó los hallazgos en octubre en su *blog* y en el *foro de seguridad antichat*, pero no se ha tenido constancia de estas actuaciones hasta ahora.

W0rm tuvo acceso a las funciones de administración del gestor de contenidos incluyendo el soporte remoto, informó a Citrix de las vulnerabilidades existentes, pero no recibió respuesta. La firma israelí de seguridad CyberInt encontró el informe, y otra vez notificó a la Citrix, sin recibir respuesta.



El 29 de enero, una vez más, *los clientes de HSBC no pudieron acceder a los servicios de banca online de la entidad debido a un ataque DDoS.*

Según los medios de comunicación, los usuarios no pudieron acceder a los frontales web de personal banking, incluyendo la aplicación de banca personal, desde las 8.30 del citado 29 de enero. Algunos usuarios reportaron que habían sido redirigidos a "www.security.hsbc.co.uk" al intentar iniciar sesión a través de su navegador.

Curiosamente el equipo de seguridad de HSBC afirmaba en redes sociales haber "defendido con éxito" el ataque a pesar de la interrupción grave sufrida.

Esta es la segunda vez que los servicios del banco no eran accesibles en lo que va de mes, ya que el 4 de enero, el Director de Operaciones pedía disculpas públicamente por la parada de más de dos días de algunos servicios TIC provocada por un corte de luz.

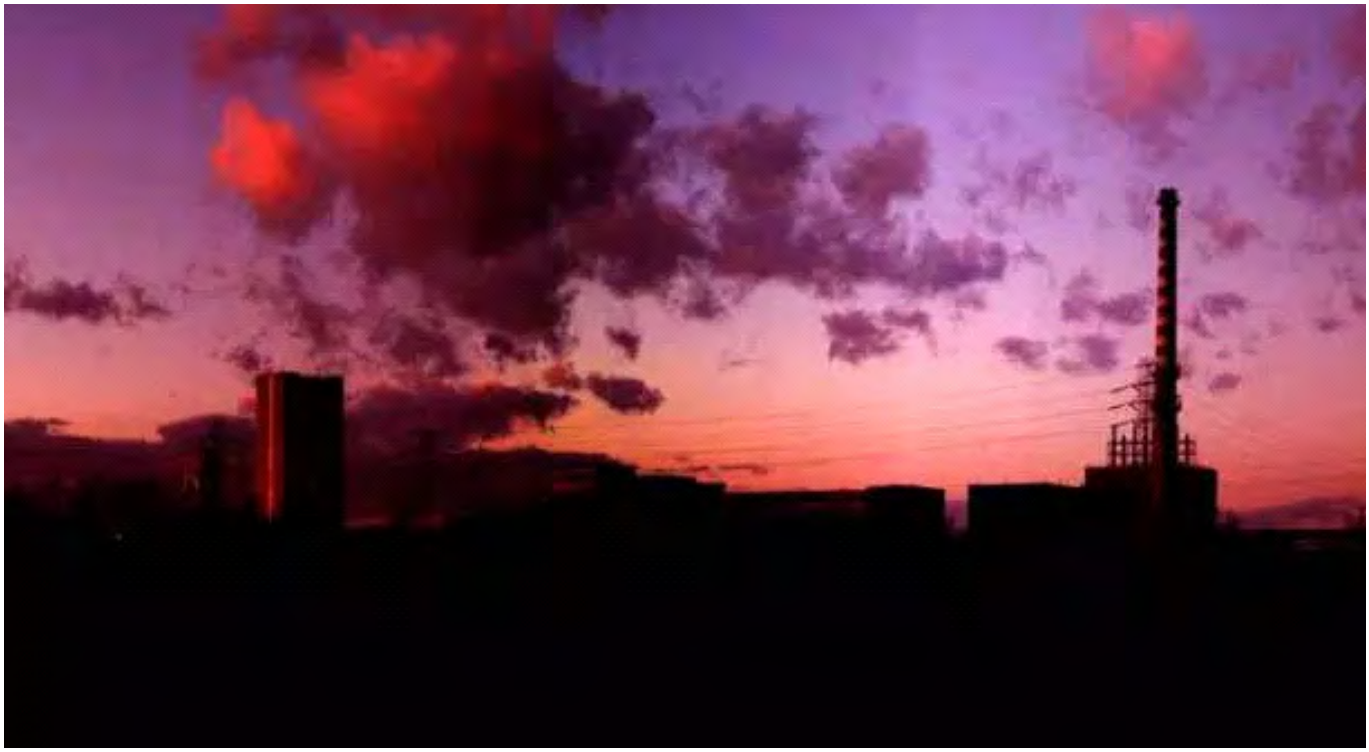
Ilustración Tweets del banco comunicando el ataque

CIBERESPIONAJE

El Ministro israelí de infraestructuras, energía y agua, Yuval Steinitz, se dirigió a los asistentes de CyberTech 2016 en Tel Aviv el pasado 26 de enero para comunicar que la *Autoridad de Servicios Públicos israelí sufrió un ataque cibernético grave.* Los actores tras el ciberataque atacaron dicha entidad mediante un malware que causó paradas en los sistemas internos.

El ministro de Energía del país, dijo que las autoridades aún están trabajando para neutralizarlo. El ataque se produce unas semanas después del perpetrado a las centrales eléctricas ucranianas basado en el malware bautizado como BlackEnergy.

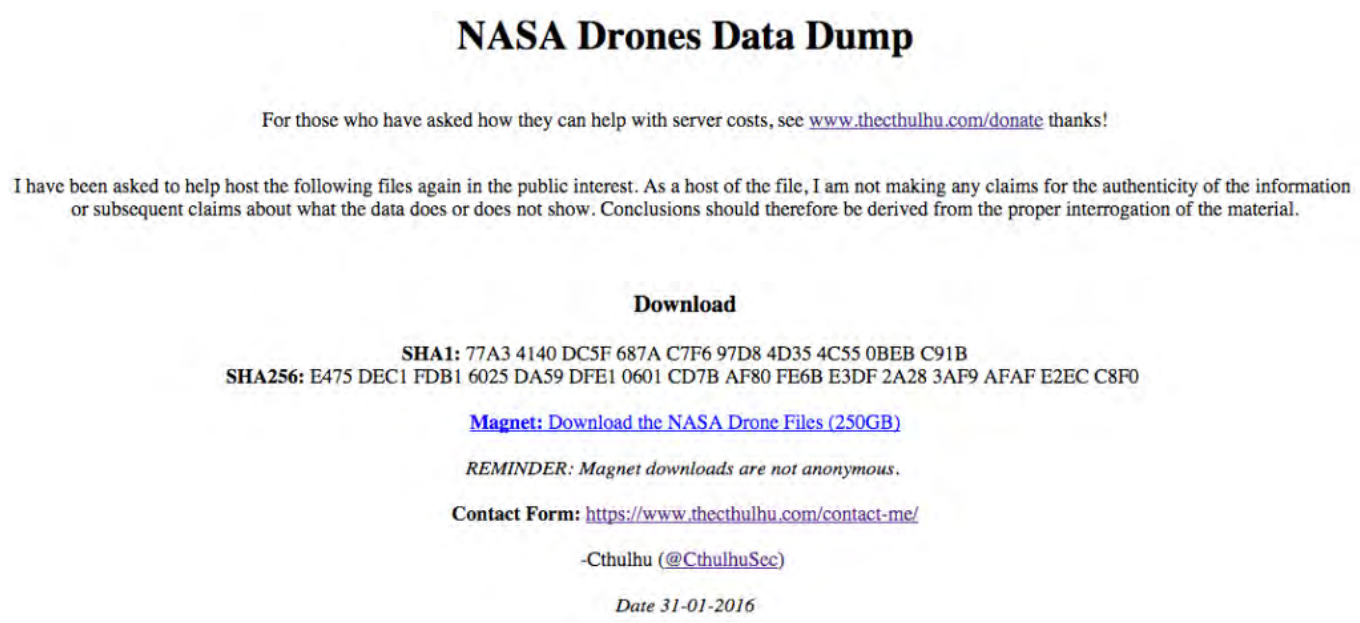
Israel, país que cuenta con uno de los sistemas de ciberdefensa más sofisticados, conocido como el Digital Iron Dome, reconoció haber sufrido uno de los mayores ciberataques de los últimos tiempos.



El Departamento Australiano de Recursos y Energía (NSW) reveló a principios de enero que en diciembre de 2015 fueron víctimas de unos ataques dirigidos aparentemente de alta sofisticación. En ese mismo periodo, la organización estaba poniendo en marcha una serie de proyectos relevantes, incluyendo un proyecto de minería de carbón en la cuenca del Shenhua.

El coste de dicho proyecto supera los 1.200 millones de dólares e implica, indirectamente, al gobierno chino. Esta circunstancia es la que sustenta las opiniones de diversos expertos de seguridad a la hora de atribuir el ataque a algún actor estatal chino que podría haber lanzado el ataque con propósitos de inteligencia, mediante la filtración de información.

Ya en el plano de los ataques con motivaciones ideológicas, políticas y religiosas, a finales de mes, *atacantes pertenecientes al grupo AnonSec publicaron más de 250 GB de datos robados de diversos sistemas informáticos de la NASA.* Entre los datos se incluyen nombres, direcciones de correo electrónico y números de teléfono de cerca de 2.414 empleados de la Agencia, así como más de 2.000 registros de vuelo y 600 canales de vídeo de la aeronave utilizada por la NASA durante sus misiones. Una vez infiltrados en los sistemas, mediante movimientos laterals, han tenido visibilidad de una gran parte de algunos segmentos de red de la NASA, habiendo *publicado hasta un mapa de red.*



NASA Drones Data Dump

For those who have asked how they can help with server costs, see www.thecthulhu.com/donate thanks!

I have been asked to help host the following files again in the public interest. As a host of the file, I am not making any claims for the authenticity of the information or subsequent claims about what the data does or does not show. Conclusions should therefore be derived from the proper interrogation of the material.

Download

SHA1: 77A3 4140 DC5F 687A C7F6 97D8 4D35 4C55 0BEB C91B
SHA256: E475 DEC1 FDB1 6025 DA59 DFE1 0601 CD7B AF80 FE6B E3DF 2A28 3AF9 AFAF E2EC C8F0

Magnet: Download the NASA Drone Files (250GB)

REMINDER: Magnet downloads are not anonymous.

Contact Form: https://www.thecthulhu.com/contact-me/

-Cthulhu (@CthulhuSec)

Date 31-01-2016

Ilustración Captura de una web en la que se puede descargar el dump de datos de la NASA

Además, los atacantes afirmaron tener bajo su control un avión no tripulado que la citada Agencia aeroespacial utiliza para ejecutar comprobaciones y muestreos en misiones de gran altitud, conocido como Global Hawk Drone.

Ilustración 4 Imagen del Global Hawk Drone de la NASA

El grupo Anonsec parece estar interesado en encontrar evidencias de la teoría de la conspiración de las estelas químicas (chemtrails en inglés). De acuerdo con dicha teoría, algunos gobiernos están usando aviones para difundir agentes químicos o biológicos para influir en el clima para diversos fines, entre ellos objetivos bélicos.

Por otra parte, el 2 de enero, el gobierno de Arabia Saudí anunció la ejecución de 47 presos por cargos de terrorismo, incluyendo un conocido clérigo chií, Sheikh Nimr Al Nimr, que fue detenido manifestarse contra el gobierno.

Ilustración Sheikh Nimr Al Nimr, clérigo chií ejecutado por Arabia Saudí

Anonymous, como protesta, lanzó un ataque de denegación de servicio distribuido sobre diversas webs gubernamentales bajo la operación #OpSaudi y #OpNimr.

Ilustración Tweet anunciando el comienzo de la operación

Ilustración Tweet mostrando algunas webs caídas

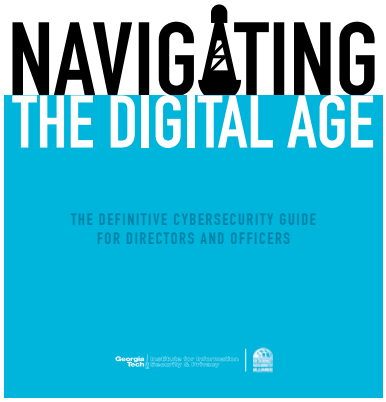
7 Recomendaciones

7.1 Libros y películas

Serie:
MR ROBOT

Sinopsis: La serie sigue a Elliot (Rami Malek), un joven hacker que sufre algún tipo de trastorno, trabaja como ingeniero de seguridad informática y usa sus habilidades para proteger a las personas por las que se preocupa. Elliot es reclutado por Mr. Robot (Christian Slater), un misterioso líder de un grupo de hackers quien quiere destruir a poderosos empresarios de multinacionales que están manejando el mundo.

paloalto | NYSE

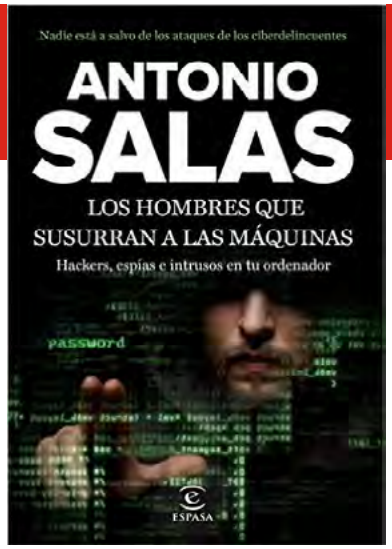


Libro:
NAVIGATING THE DIGITAL AGE

Autor: : Matt Rosenquist (editor)
Num. Paginas: 369
Editorial: CAXTON Business & Legal
Año: 2015
Precio: FREE
Sinopsis: Este libro, patrocinado por la empresa tecnológica Palo Alto y el New York Exchange Stock (NYSE), pretende ser la guía definitiva para los ejecutivos con competencias en materia de ciberseguridad. Para ello, cuenta con los testimonios de un centenar de directivos de las principales empresas tecnológicas del mundo.

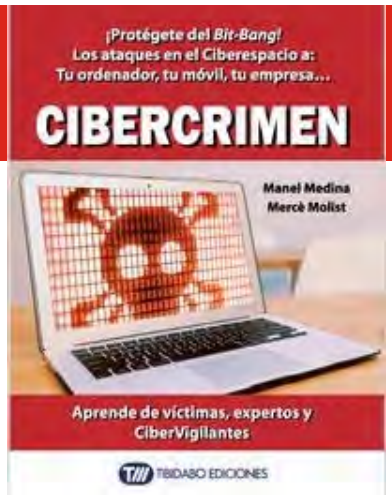
Libro:
CONNECTIVITY WARS

Autor: : Mark Leonard (editor)
Num. Paginas: 224
Editorial: ECFR
Año: 2016
Precio: FREE
Sinopsis: Este libro analiza el campo de batalla del futuro que, según sus actores, no serán los entornos convencionales del conflicto (mar, tierra, aire y espacio) sino tendrán como protagonistas a Internet, el movimiento de personas o la guerra económica, entre otras.



Libro:
LOS HOMBRES QUE SUSURRABAN A LAS MAQUINAS

Autor: Antonio Salas
Num. Paginas: 220
Editorial: Espasa Calpe
Año: 2015
Precio: 12,50 Euros
Sinopsis: Durante los últimos años el autor ha conocido a hackers de sombrero blanco, gris y negro, a ciberactivistas y ciberpolicías. Así como a espías que utilizan las redes para robar información y a los yihadistas que distribuyen en ellas su propaganda. Igualmente, ha explorado la Deep Web y el negocio de la pedofilia; y ha comprendido cómo la ciberdelincuencia golpea a cualquier persona sin distinción. Este libro recoge todas estas vivencias.



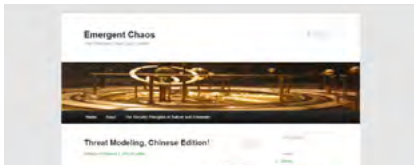
Libro:
CIBERCRIMEN

Autor: Manel Medina y Merce Molist
Num. Paginas: 552
Año: 2015
Precio: 15,20 Euros
Sinopsis: Guía sobre los riesgos y peligros que podemos encontrar en nuestras actividades digitales, escrito con la precisión de experto que aporta Manuel Medina, con la colaboración de Pedro Pablo Pérez García, y con textos muy asequibles a cualquier nivel escritos la periodista y divulgadora de temas de seguridad informática Mercé Molist.

7.2 Webs recomendadas

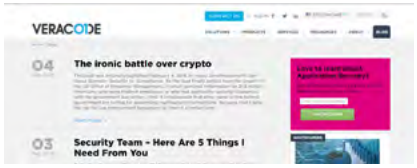
http://dankaminsky.com/
Blog de Dan Kaminsky, un reconocido investigador en materia de ciberseguridad, que durante los últimos años ha asesorado a multinacionales como Cisco, Avaya o Microsoft.

http://emergentchaos.com/
Este blog, creado en 2004 por Adam Shostack, contiene cientos de artículos sobre ciberseguridad y privacidad tratados de un modo inteligible para todos los lectores que se acerquen a él.

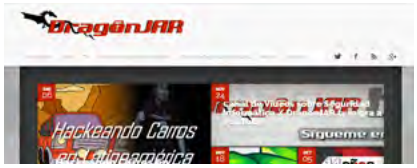


https://blog.elearnsecurity.com/
Este blog pertenece a la plataforma eLearnSecurity que ofrece cursos de seguridad dirigidos a los profesionales de la seguridad TIC.

https://www.veracode.com/blog/
Blog de la empresa de seguridad de aplicaciones VERACODE.



http://www.dragonjar.org/
Una de las comunidades en materia de ciberseguridad más grandes en habla hispana fundada por Andrés Restrepo.

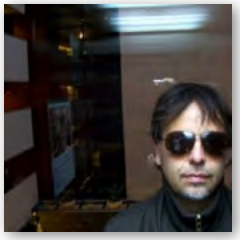


http://www.daboblog.com/
Blog personal de David Hernández (aka. Dabo), este es “el sitio” por excelencia para todos los usuarios de GNU/Linux y específicamente Debian.

7.3 Cuentas de Twitter

@tomquillin

@RonDeibert



@seanlawson

@MeleStefano

@PatrickCMiller

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
5 al 6 de febrero	Tenerife	Hackron	Hackron III	www.hackron.com
9 de febrero	Madrid	CIC	Systems Security Day 2016	http://www.systemssecurityday.com/
11 de febrero	Madrid	IDC	Forum ciberseguridad	http://www.cvent.com/events/idc-ciberseguridad-2016-madrid-spain/event-summary-2c805a25b5a149b287be3d44e1e02b87.aspx
12 febrero	Madrid	DPI- ISMS Forum	VIII Foro de la Privacidad	https://www.ismsforum.es/evento/636/viii-foro-de-la-privacidad/
12 al 13 de febrero	Cuenca	UCLM	MorteruelоCON	www.morteruelo.net
17 al 18 de febrero	Granada	Telefonica	Hackathon Sinfonier Project	https://docs.google.com/forms/d/1CpMKq9WEvqjaaslEK0vgi04MRrBArHbBgD3RVafT0nw/viewform?c=0&w=1
23 al 26 de febrero	Madrid	IFEMA	SICUR 2016	http://www.ifema.es/sicur_01/
26 de febrero	Pozuelo de Alarcón	SoftCare	CYBERSECURITY SAM ENGAGEMENT	http://www.softcare.es/emailing/cyberscurity/index-invitacion.html
22 al 25 febrero	Barcelona	GSMA	Mobile World Congress 2016	https://www.mobileworldcongress.com/
25 febrero	Madrid	Ediciones Coda	El despegue de los Seguros de Responsabilidad Cibernética	https://revistasic.es/index.php?option=com_content&view =article&id=1488&Itemid=1331
29 febrero al 4 marzo	San Francisco	RSA	RSA 2016 Security Conference	http://www.rsaconference.com/

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