JUNIO 2016 / Nº 15

CIBER elcano

REAL INSTITUTO elcano ROYAL INSTITUTE

Desarrollado por:

THIBER

INFORME MENSUAL DE CIBERSEGURIDAD

REAL INSTITUTO
elcano
ROYAL INSTITUTE

Copyright y derechos:

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
DIUX 2.0: Gestionar el cambio para lograr la superioridad tecnológica

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

Fuente: *www.defense.gov*

El pasado 11 de Mayo, el Secretario de Defensa Ashton Carter anunciaba el relevo de George Duchak al mando de la *Defence Innovation Unit Experiment (DIUX)* – tan solo 9 meses después de haberse puesto en marcha este experimento patrocinado por el Pentágono –y presentaba el DIUX 2.0, que será dirigido por *Raj Sash*, un militar en la reserva, ex piloto de F-16 y hasta hace unas semanas Director de Estrategia de la compañía PaloAlto.

Recordemos que la DIUx *fue creada en julio de 2015* en el marco de la *Defense Innovation Initiative* para generar nuevas capacidades militares y el *Long Range Research and Development Plan* para apoyar las propuestas tecnológicas de la industria civil estadounidense, madurarlas e integrarlas en los sistemas armamentísticos claves para la Tercera Estrategia de Compensación (Third Offset). Recuérdese que hoy en día la mayoría de los avances tecnológicos no proceden de la industria militar sino de la civil, razón por la que todos los planes de desarrollo de nuevas capacidades militares vinculados con la Tercera Estrategia de Compensación se basan en la *colaboración público-privada.* Es por ello que el nuevo DIUX deberá disponer de los medios, capacidades y conocimientos necesarios para contribuir en el mantenimiento del liderazgo tecnológico, especialmente el relacionado con el ciberespacio.

Durante su comparecencia, Carter anuncio que la la DIUX 2.0 deberá *"tener una estructura organizativa y trabajar como cualquier start-up de Silicon Valley".* Del mismo modo, aseguró que *"..una de las lecciones aprendidas durante los primeros meses de vida del DIUX ha sido que el Departamento de Defensa(DoD) no es lo suficientemente rápido y ágil."* Aunque Carter ha defendido que DIUX2.0 no es una iteración perfectiva del proyecto sino una nueva fase del mismo que afianzará y mejorará el proyecto, parece evidente que los resultados del DIUX 1.0 no fueron los esperados, en parte porque Duchack, quien seguramente comprendió la filosofía de emprendimiento de Silicon Valley, fue incapaz de gestionar el experimento de manera autónoma, ahogándolo en los tediosos procedimientos administrativos de un gigante como es el Departamento de Defensa. Sea como fuere, el nuevo DIUX – que abrirá nueva sede en Boston en los próximos meses – reportará directamente al Secretario de Defensa para intentar asegurar su éxito.

El anuncio del DIUX 2.0 se produce a tan solo unos meses de las elecciones presidenciales en los Estados Unidos. En consecuencia, a principios de 2017 un nuevo Secretario de Defensa será el encargado de evaluar el nivel de madurez y rendimiento del experimento. No cabe duda de que Sash tiene ante sí un gran reto.

En definitiva, el lanzamiento del DIUX 2.0 ha puesto de manifiesto tanto la dificultad de las grandes organizaciones como el Pentágono para gestionar el cambio, pero también su flexibilidad a la hora de lanzar esta nueva iniciativa. Es necesario que las organizaciones aprendan de sus errores y asuman que los ciclos de desarrollo tradicionales son completamente irrelevantes e inasumibles cuando analizamos el ciberespacio.

"Es necesario que las organizaciones aprendan de sus errores y asuman que los ciclos de desarrollo tradicionales son completamente irrelevantes e inasumibles cuando analizamos el ciberespacio"

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL Algunas consideraciones sobre el origen y los retos de la directiva NIS

AUTORES: Ángel Vallejo. Responsable de Relaciones Institucionales, THIBER.
Socio de MAIO LEGAL.

Bajo estas líneas se recogen algunas consideraciones sobre el origen y los retos de una Directiva cuyo alumbramiento despierta por igual expectativa sobre su efectiva implantación así como recelo sobre los sujetos obligados a cumplirla:

a).- En términos cibernéticos, un período de tres años no está lejos de considerarse una eternidad. Pues bien, hace más de tres años, el 7 de febrero de 2013 la Comisión Europea formalizó la propuesta de Directiva relativa a la seguridad de las redes y la información (conocida como Directiva NIS por sus iniciales en inglés, *Network and Information Systems*). Al mismo tiempo la Comisión había comunicado al Parlamento Europeo y al Consejo Europeo, entre otras instituciones, la aprobación de la Ciber Estrategia Europea como base de lo que habría de venir después.

La Comisión puso sobre la mesa en 2013 cuestiones evidentes y otras que no lo eran tanto. Europa, como otras tantas unidades económicas y sociales perteneciente al primer mundo desarrollado, basaba ya entonces la mayoría de su actividad comercial, política y empresarial en las tecnologías de la información y la comunicación (TIC).

La transversalidad de las TIC y su cualidad de ser vehículo para la práctica totalidad de la actividad actual incluso en el ámbito personal en Europa hacen necesario exigir al legislador comunitario que se emplee a fondo en emitir normas adecuadas con especial velocidad y acierto. Las TIC y el sustrato físico de las mismas son ya desde hace años el medio a través del que buena parte del comercio se negocia o se ejecuta, del que se ejercitan derechos fundamentales y constituyen también la herramienta con la que se desarrolla un muy importante porcentaje de las relaciones de carácter personal.

Los beneficios que el mundo digital puede producir para la mayoría de las sociedades, especialmente para aquellas que, como la nuestra y las de nuestro entorno europeo, gozan de elevados niveles de desarrollo económico, social y tecnológico, no vienen solos. En efecto, tales beneficios presentan inevitablemente vulnerabilidades que, por

afectar a derechos esenciales y a la diaria actividad social y económica, son susceptibles de generar daños de consideración.

Y el origen de tales riesgos se hace cada vez más amplio, no limitándose ya a la ciberdelincuencia. En orden de magnitud distinto nos enfrentamos ahora a riesgos relacionados con actividades de estados soberanos que (de momento de manera no declarada) emprenden campañas de acoso o de ataque directo contra ciudadanos de otros países, contra sus compañías o incluso contra otros estados.

Es reseñable el incremento de los casos de espionaje económico y lo es también el de los casos en que las autoridades de determinados países emplean los medios del ciberespacio para vigilar y controlar de manera ilegítima a los ciudadanos. En este punto es necesario oponer como contrapeso el fomento de la libertad en línea y un escrupuloso respeto de los derechos fundamentales en la red.

"Es reseñable el incremento de los casos de espionaje económico y lo es también que las autoridades de determinados países empleen los medios del ciberespacio para vigilar y controlar de manera ilegitima a los ciudadanos"

Como adelantaba la propuesta de la Comisión, la UE debe garantizar que los mismos derechos que rigen en el "mundo físico" sean idénticamente protegidos en la red. Cualquier desarrollo legislativo que obvie ese aparentemente indiscutible concepto de universalidad de tales derechos (con independencia del medio en el que se ejerzan) significará dar carta libre a un retroceso en los estándares de los derechos adquiridos en la UE.

Uno de los activos que las citadas instituciones consideraron que estaba en riesgo, probablemente el más intangible, era la confianza de los consumidores europeos y de la sociedad europea en su conjunto. Socavar tal confianza supondría afectar a la consecución de proyectos de tan hondo calado como el Mercado Único Digital Europeo.

Sobre esa base, y debido a la más que evidente disparidad en las capacidades y preparación en el ámbito de la seguridad de las redes y la información, resultaba claro que una aplicación voluntaria de acuerdos sobre estándares cibernéticos por parte de los Estados miembros no podría generar la protección suficiente para afrontar los incidentes y riesgos de ciberseguridad. Las cadenas rompen por el eslabón más débil, de modo que de nada valdría que un Estado miembro contase con las mejores capacidades y protocolos cibernéticos si otro Estado, interconectado necesariamente con el primero, no estuviese en idéntica o similar situación de desarrollo.

Es innegable que la UE ha sido puntera y ha culminado avances esenciales en la mejora de la protección de sus ciudadanos frente a la ciberdelincuencia, entre los que destacan el establecimiento del Centro Europeo de Ciberdelincuencia (IP/13/13), la propuesta de legislación sobre los ataques informáticos (IP/10/1239) y el lanzamiento de una alianza mundial contra los abusos sexuales a menores en línea (IP/12/1308).

También se ha operado con prontitud en relación con la protección de datos. El pasado 4 de mayo se publicó el nuevo Reglamento del Parlamento y del Consejo 2016/679, de 27 de abril, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos. El Reglamento será directamente aplicable y de obligado cumplimiento en todos los Estados miembros de la Unión Europea transcurridos dos (2) años de su entrada en vigor, es decir, el 25 de mayo de 2018.

Sin embargo, se hizo evidente la necesidad de una normativa de base que protegiera el vehículo esencial que constituían las TIC en Europa para la protección y el desarrollo de los derechos fundamentales en el ejercicio de las actividades cibernéticas legítimas, del tipo que fueran. Por mucho derecho teórico y mucho desarrollo deseado de las cuestiones de fondo que estuviera presente, si no se garantizaba el buen funcionamiento de su sustrato cibernético, del medio en el cual se actúa, la realidad podría acabar pareciéndose muy poco al estándar teórico europeo.

Tal y como acertadamente manifestó Neelie Kroes, vicepresidenta de la Comisión responsable de la Agenda Digital, *"cuanta más gente dependa de Internet, más gente dependerá de que la red sea segura. Una red*

segura protege nuestros derechos y libertades y nuestra capacidad de ejercer actividades económicas. Ha llegado el momento de coordinar nuestra acción: el coste de la inacción es mucho más elevado que el de la acción".

Con lo anterior en mente, cuando se llevó a cabo un estudio comparativo de los procesos aplicados por los proveedores de servicios esenciales y por los encargados de gestionar las infraestructuras críticas se llegó a la conclusión (nada sorprendente, como es lógico) de que no todos ellos en cada uno de los Estados miembros venían obligados de igual manera a i).- adoptar las mismas medidas de seguridad, ii).- gestionar el riesgo tecnológico y iii) comunicar ciberincidentes a las autoridades competentes.

Con este panorama, la única posibilidad de futuro era imponer un enfoque común sobre la seguridad de las redes y la información y es ahí donde tiene su origen la Directiva NIS, que bebe directamente del texto de la Ciberestrategia Europea que acertadamente se tituló *"Un ciberespacio abierto, protegido y seguro".*

b).- El resultado de todo el largo proceso legislativo europeo ha sido que tras la adopción por el Parlamento en primera lectura de su posición al respecto el 13 de febrero de 2014, el Consejo ha adoptado el 17 de mayo de 2016, su posición sobre dicha Directiva, también en primera lectura, después de que en 2015 salieran a la luz las graves diferencias entre Consejo y Parlamento en relación con determinados extremos relevantes del borrador de la norma. En estos momentos, el único trámite pendiente para que la Directiva NIS sea una realidad es la aprobación del acto jurídico por el PE en segunda lectura, tras lo cual la norma estará lista para su entrada en vigor, lo que probablemente ocurra en agosto de 2016.

c).- El carácter de Directiva de la nueva norma no resulta ser cuestión menor. Como es sabido, los Reglamentos europeos tienen alcance general, son obligatorios en todos sus elementos y resultan directamente aplicables en cada Estado miembro, con la particularidad de que cualquier ciudadano europeo puede exigir su cumplimiento y acudir directamente ante los tribunales nacionales en caso de que considere que el contenido de la norma se esté incumpliendo.

"Una red segura protege nuestros derechos y libertades y nuestra capacidad de ejercer actividades económicas."

Las Directivas (la NIS lo es) por el contrario, no constituyen derecho directamente aplicable en los estados miembros, sino que necesitan de una transposición normativa en cada uno de los Estados miembros para que produzcan los efectos perseguidos.

d).- En términos generales la Directiva obliga a los Estados miembros a definir los operadores esenciales de servicios de Energía, Transporte, Banca y Salud y también a los proveedores claves de servicios digitales tales como buscadores y proveedores de *cloud computing.*

Definidos tales operadores, los Estados impondrán a los mismos la obligación de tomar las medidas de seguridad necesarias y la de informar de incidentes significativos a las Autoridades Nacionales que se definan, a su vez, como competentes. En este sentido cada país.

1. designará una Autoridad Nacional competente para gestionar la materia NIS

2. implementará un Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT, por su denominación en inglés, *Computer Security Incident Response Team).*

Los Estados miembros tendrán que definir la estrategia nacional y el plan de cooperación de Seguridad de las Redes y de la Información, para lo cual contarán con la coordinación de la Agencia Europea para la Seguridad de las Redes y de la Información (ENISA, por su denominación en inglés, EU Agency for Network and Information Security) de cara al trabajo conjunto y la intercomunicación de los distintos CSIRTs. Con carácter más genérico, habrá de implementarse un plan de cooperación entre los Estados Miembros de información de los posibles riesgos e incidentes de ciberseguridad.

Nuestro país cuenta ya con una Estrategia de Seguridad Nacional y una Estrategia de Ciberseguridad, de modo que es previsible que el esfuerzo necesario (que no es poco) sea el de adaptar esta segunda a los dictados de la Directiva, frente al mayor desempeño que será exigible a los países que ni siquiera tuvieran desarrollada su ciberestrategia.

Bajando de lo público a lo privado, y particularmente a lo empresarial, de la Directiva NIS se derivan efectos muy relevantes para las compañías del ámbito cibernético, si bien la

norma no será extensiva a todas y cada una de estas compañías.

En primer lugar, y esto no es en absoluto baladí, cada compañía habrá de concluir si la Directiva le resulta aplicable. Como antes se dijo, la NIS tiene como destinatarios finales (del tipo no estatal, lógicamente) a los operadores de servicios esenciales y a proveedores de servicios digitales, como los correspondientes a los sectores de Energía, Transporte, Financiero, Hidrológico, Administración Publica y Salud, las infraestructuras digitales, los negocios de comercios online, los buscadores de la red y los servicios de *Cloud Computing.*

Extrañamente, la Directiva no tiene vocación de afectar a compañías de hardware o software ni tampoco son sujetos de la NIS las consideradas pequeñas y medianas empresas, asunto que desde el primer momento ha originado una interesante polémica que viene avivándose en los últimos meses.

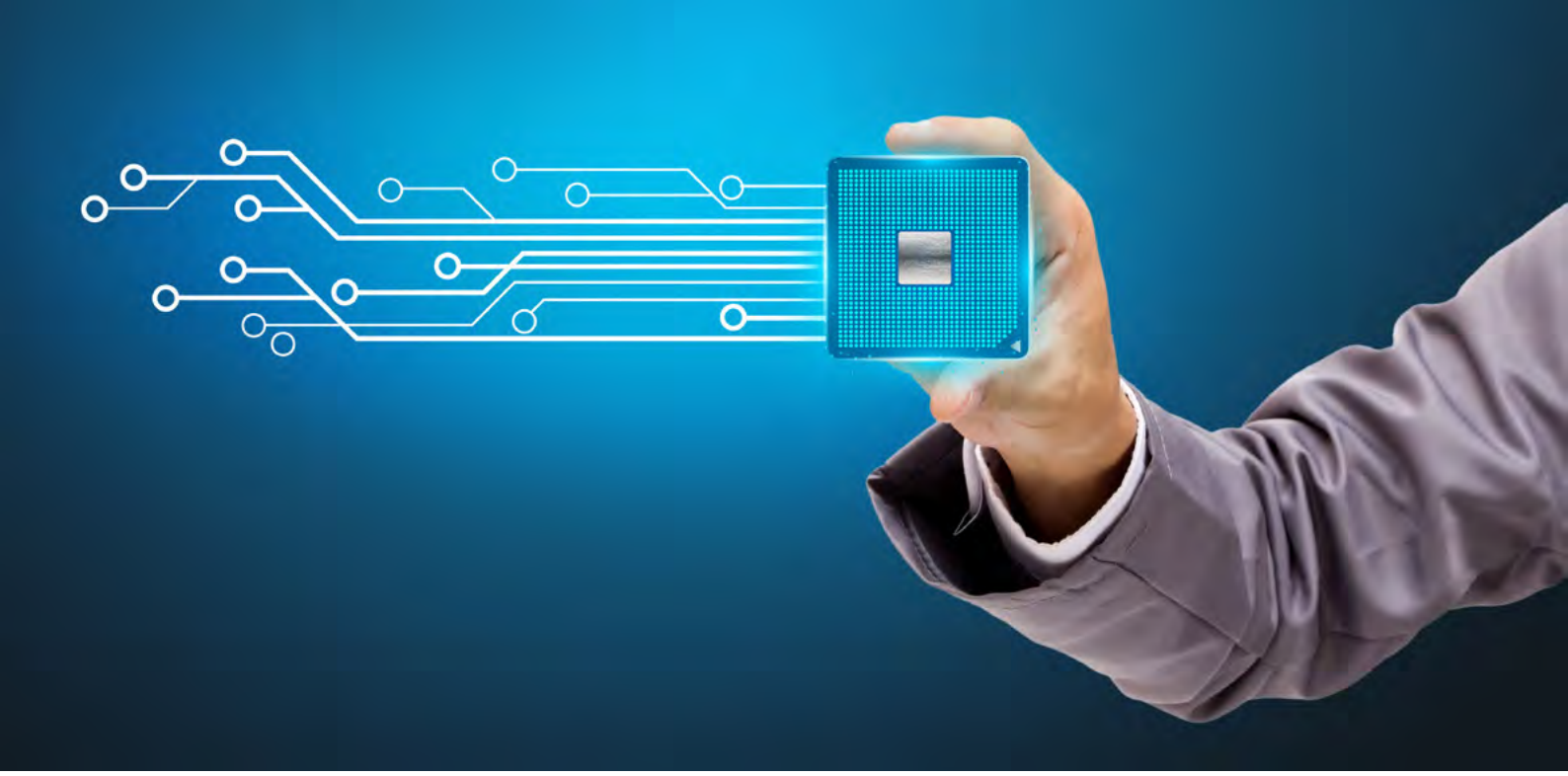
Si se encuentra entre los sujetos destinatarios de las obligaciones de la Directiva, deberá atenerse a la Ley nacional por medio de la cual el Estado miembro donde la misma tenga su oficina principal transponga la NIS en su territorio. Recordemos aquí lo antes expuesto en el sentido de que las Directivas no son directamente aplicables en el territorio de los Estados miembros (al contrario que los Reglamentos europeos).

"NIS obliga a los Estados miembros a definir los operadores esenciales de servicios de Energía, Transporte, Banca y Salud y también a los proveedores claves de servicios digitales tales como buscadores y proveedores de cloud computing."

Y ese cumplimiento de la ley nacional obligará a la compañía a conocer cuál es la Autoridad nacional a la que reportará los incidentes de ciberseguridad y también cuál es la Autoridad que en su caso habrá de imponer las sanciones derivadas del incumplimiento legal.

Como es lógico, contando ya con el cumplimiento de las cuestiones formales, la compañía en cuestión tendrá que poner en practica la medidas técnicas y organizativas imprescindibles para proteger su información y sus redes (esta es la razón esencial de la NIS). Tales medidas tienen que garantizar las capacidades que permitan una adecuada gestión de los riesgos y amenazas en la seguridad de las redes y los sistemas de información propios. Y dado que incluso con la gestión de riesgo citada es posible que se produzcan ciberincidentes, la compañía ha de implementar un proceso efectivo para notificarlos al CSIRT nacional.

Huelga decir que uno de los objetivos (intangible, pero no por ello menos importante) de la Directiva es conseguir que las compañías de todos los Estados miembros generen una cultura de la gestión del riesgo tecnológico, adoptando las medidas que sean apropiadas y proporcionales para garantizar la seguridad de su información y sus redes. Eurostat reveló que, hasta enero de 2012, solo el 26 % de las empresas de la UE había definido una política formal de seguridad de las TIC.



Apuntaremos aquí que uno de los pilares de la adecuada gestión de este tipo de riesgos es la transferencia vía aseguramiento en los casos en que sea necesario[1].

e).- Incluso con la inminente entrada en vigor de la Directiva NIS, el estado del arte afronta unos importantísimos retos derivados, por un lado de la constante y rápida trasformación de las TIC y, por otro, del modo en que los Estados miembros y las propias instituciones de la UE ejecuten los planes que contiene la propia Directiva. A ellos nos referimos a continuación.

Lo primero que está por ver (aunque hasta el momento su desempeño pueda calificarse como de satisfactorio) es qué grado de efectividad despliega la Agencia de Seguridad de las Redes y de la Información (ENISA) respecto de las tareas adicionales que la Directiva le otorga. Es cierto que esta agencia ha comenzado ya a preparar y coordinar la aplicación de la norma NIS, incluso antes de la adopción de la posición del Consejo en mayo de 2016. De hecho, el 5 de abril de 2016 se produjo la primera reunión informal de la red de equipos de respuesta a incidentes de seguridad informática (CSIRT), creada en virtud de la Directiva, y muy recientemente se celebró de una segunda reunión en Riga el 10 de mayo.

En otro orden de cosas y a pesar de que existe una mayor coordinación de la que algunos ciudadanos consideran, no puede descartarse que la transposición en cada Estado miembro derive en planes de ciberseguridad diferentes (aunque no contarios a la Directiva, lógicamente) que prevean medidas de ciberseguridad distintas en cada país. Los diferentes niveles de madurez en el ámbito de la ciberseguridad existentes en cada Estado miembro puede generar cierta fragmentación en las definiciones del plan de cada país. Igual que ocurre con las políticas de protección de

[1] Ver en este punto el documento el documento de THIBER, the cybersecurity think tank titulado “CIBERSEGUROS: La transferencia del ciber riesgo en España” disponible *aqui*.

datos (materia en la que España es percibida como una jurisdicción especialmente inflexible) es inevitable que unos Estados miembros sean más estrictos en la interpretación que otros. El reto en este punto es evidente.

En un ámbito radicalmente distinto del anterior, las pequeñas y medianas empresas, al no ser destinatarias naturales de la Directiva, podrían quedar como el eslabón más débil de la cadena y generar un serio problema, En efecto, no es nueva la consideración del *supply chain risk* como un puntal esencial en los sistemas de gestión del riesgo, y da la impresión de que, atendido el grado de innovación tecnológica y las capacidades de procesamiento de algunas empresas que, por tamaño, no entran dentro de las previsiones de la Directiva NIS, la gestión del riesgo proveedor va a tener que optimizarse para evitar la concreción de riesgos que puedan llegar a ser sistémicos, atendido el hecho de que las PYMES suponen el mayor porcentaje de compañías que utilizan infraestructuras NIS.

Otro reto común para todos los países de la UE es el de la coordinación entre la Autoridad Nacional Competente (NCA) y el CSIRT nacional en cada Estado. No está definitivamente claro cuáles serán los poderes concretos que ambas instancias tendrán otorgados y esto, junto con la posibilidad de que algunos operadores esenciales terminen viéndose sujetos a la obligación de notificación simultánea a distintos supervisores nacionales o de ámbito europeo generará sin duda ineficiencias que habrán de ser inmediatamente detectadas y corregidas.

Por último, y entendemos que de capital importancia, nos referimos a ENISA. Hemos adelantado que la agencia es destinataria de nuevas e importantes funciones de acuerdo con el texto de la Directiva, que la contempla como un actor fundamental para el aseguramiento de la infraestructura de las TIC en toda la UE.

ENISA viene organizando ejercicios periódicos de crisis con el fin de formar ciber expertos y potenciar la cooperación entre ellos en materia de buenas prácticas, es decir, se ha puesto el foco en la agencia como facilitador y gestor esencial. Entre otras funciones, a ENISA le corresponderá coordinar la red CSIRT a nivel europeo. Ya desde el año 2005 ENISA cuenta con una red de CSIRT nacionales y gubernamentales que se utiliza para potenciar la confianza y permitir el intercambio de información. También forma parte, junto con los miembros de las distintas NCA y la Comisión, del denominado Grupo de Cooperación.

Queda por ver si tan relevante actor es destinatario no solo de la consideración política que supone verse designado como *key player* en el seno de la política NIS europea, sino también si, realmente, su desempeño teórico va a contar con los fondos necesarios para tan necesario fin.

3 Entrevista al Col. Manuel Navarrete.

Responsable del Centro Europeo Contra el Terrorismo (ECTC) de EUROPOL

1. Como responsable del Centro Europeo Contra el Terrorismo (ECTC) de EUROPOL ¿podría indicarnos cuáles son las principales competencias del centro? ¿Cuál es su ámbito de actuación?

La iniciativa de crear el Centro Europeo Contra el Terrorismo (ECTC) nace, en parte, de la propia Europol para vertebrar parte de su estrategia general, mejorar el intercambio de información, ofrecer un análisis más profundo de las capacidades existentes en el ámbito de inteligencia financiera, lucha contra el crimen organizado o el terrorismo y ser mucho más cercanos a los estados miembros. Europol está trabajando para que sus productos y sus analistas sean más accesibles, siendo el capital humano de la organización un punto clave del valor que ofrece.

El ECTC aporta una mayor coherencia en las actuaciones en la lucha contra el terrorismo. Se ha identificado como acción necesaria potenciar el intercambio de información, por lo que se ha desarrollado una herramienta específica de comunicación segura denominada CT SIENA, o Siena para Contraterrorismo, para que las 43 autoridades competentes en terrorismo que actualmente usan la herramienta – tanto europeas como internacionales como Estados Unidos – puedan usar esta plataforma para intercambiar información. Por otra parte, se está haciendo énfasis en mejorar las capacidades de análisis de información provenientes tanto de los propios miembros como los generados por la propia Europol, mediante las diversas

bases de datos existentes (crimen, terrorismo, cibercrimen, etc.). Se ha creado una unidad específica para trabajar contra el terrorismo online, la Internet Referral Unit (EU IRU), que actúa en el ámbito de la prevención al coordinar a los estados miembros y los diferentes proveedores de acceso a internet (ISPs) y proveedores de servicios online para ponerles de manifiesto cómo los terroristas hacen un uso abusivo de sus plataformas y servicios para difundir propaganda o realizar labores de radicalización y captación, solicitando la retirada de contenidos o eliminación de determinados perfiles de usuarios.

Por último, el ECTC actúa como un elemento dinamizador de colaboración entre los distintos cuerpos especializados en la lucha contra el terrorismo, creando una red de expertos que están en permanente contacto

con los cuerpos policiales nacionales. Por ejemplo, esta red colaboró de forma activa tras los atentados de París y de Bélgica, y ahora mismo está activamente involucrada con agentes en el terreno para ofrecer un nivel de protección adicional durante el desarrollo de la Eurocopa. Igualmente, esta red también se está involucrando en otras iniciativas como la identificación del uso de las redes de inmigración ilegal para introducir terroristas en la zona europea o la elaboración de una lista de los denominados *foreign fighters.*

2. Para el desarrollo de esas actividades, ¿se cuenta con medios técnicos y personales propios o también con colaboración de las diversas naciones europeas y de la industria privada? ¿Existen herramientas y programas eficaces y efectivos para la colaboración público-privada en Europol en la lucha contra el terrorismo en todas sus vertientes, incluida la cibernética?

Europol tiene un staff permanente seleccionado a través de los mecanismos de gestión de personal de la propia organización, con diversos perfiles técnicos, contando con personal altamente cualificado. Al mismo tiempo Europol también cuenta con personal externo aportado por los estados miembros en dos modalidades: oficiales de enlace permanentes (más de 200) o expertos aportados por las naciones (oficiales cedidos), proporcionando una mayor vinculación con el estado miembro en determinados proyectos. Así pues, Europol cuenta con una presencia equilibrada entre staff permanente especializado con oficiales de enlaces y expertos en colaboraciones puntuales.

"Europol ha creado la Internet Referral Unit (EU IRU), una unidad especifica para trabajar contra el terrorismo online"

3. El nuevo Centro Europeo Contra el Terrorismo (ECTC) combina diversas capacidades de información e inteligencia ¿podría indicar cuáles son las principales?

Europol tiene dos funciones fundamentales:

1. Facilitar el intercambio de información, como puede ser a través del sistema SIENA, entre agencias de inteligencia y cuerpos policiales identificados por los estados miembros en el ámbito del terrorismo, ya que existe cierta heterogeneidad a nivel europeo en cuanto a modelos de estructuración nacional en la lucha contra el terrorismo.

2. Apoyo analítico, buscando lo que en el ámbito de Europol se denomina hits management o gestión de cruces de datos, es decir, coincidencias en operaciones e investigaciones que puedan ayudar a los países en sus actuaciones. Europol actúa además como colaborador en el grupo de inteligencia de la Unión Europea, liderado actualmente por Holanda. Este grupo es el resultado de una creciente necesidad de coordinar las actuaciones policiales y de inteligencia.

4. ¿Con qué tipo de entidades europeas y nacionales tiene que colaborar el Centro para el desarrollo de sus funciones nominales?

Entidades nacionales que cada Estado Miembro designa; autoridades competentes de ámbito internacional o estados extracomunitarios (Australia, Suiza, Estados Unidos, Colombia, Noruega, etc.) u otras agencias europeas como Frontex (con la cual se tiene una gran colaboración), o internacionales como INTERPOL.

5. ¿Existen mecanismos ágiles de coordinación desde Europol con las fuerzas y cuerpos de seguridad nacionales europeas? ¿y con otros organismos y agencias internacionales?

El mecanismo de intercambio de información por excelencia es la red de oficiales de enlace presentes en la organización. Desde el punto de vista de una entidad como Europol, el secreto de su agilidad no sólo reside en contar con el mejor *staff*, sino también con la mejor "conectividad" en la relación con los países.

6. Hemos asistido en los últimos tiempos a un uso incremental y cada vez más sofisticado de los medios digitales y redes sociales, entre otros, por parte de grupos terroristas e integristas radicales de diversa índole. ¿Qué respuesta se prevé desde el Centro para hacer frente a esta amenaza? ¿Disponemos de medios para hacer frente a la propaganda yihadista en internet?

Europol en un actor más en la lucha contra los procesos de radicalización y está desarrollando contranarrativas en el marco de otros proyectos europeos y en colaboración con otros actores sociales. Más concretamente, Europol trabaja en dos campos complementarios: por un lado, la prevención de la difusión de la propaganda terrorista mediante una unidad específicamente diseñada para tal efecto, la citada IRU, que se encarga de monitorizar redes sociales, identificar perfiles violentos, observar la propaganda terrorista y reducir – en colaboración con los proveedores de Internet – la exposición a dicha propaganda. Por otro lado, la investigación, donde estamos rastreando Internet e incorporando técnicas y procedimientos propios de la investigación de la cibercriminalidad en nuestra caja de herramientas para combatir el terrorismo.

7. Desde un punto de vista prospectivo ¿cuál cree que será el panorama de amenazas terroristas en el ámbito ciber que veremos en los próximos años? ¿Estarán los ciudadanos y naciones europeas preparados para hacer frente a estos nuevos vectores de amenazas como el ciberterrorismo? ¿será esta última una amenaza real a medio plazo?

Todos los países están tomando medidas para mitigar la amenaza y los riesgos derivados de ella. En España existe un plan para la protección de infraestructuras críticas y en el marco de la Unión Europea disponemos de un programa similar para limitar la exposición y reducir el impacto de un ciberataque terrorista contra una infraestructura de estas características. En materia legal también estamos haciendo importantes avances con la discusión de una nueva Directiva para combatir el terrorismo que pretende considerar los ciberataques como actos de terrorismo. Finalmente, también estamos estudiando las actividades que pueden realizar grupos terroristas en Internet para atacar otras infraestructuras y redes de comunicación.

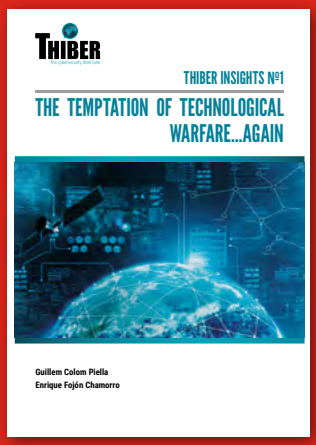
En definitiva, la evolución técnica de Internet es muy rápida y no sólo ofrece oportunidades a los ciudadanos, sino también a otros actores que pueden valerse de Internet para fines ilegítimos. Es por ello que es fundamental priorizar la prevención, la investigación y la mitigación de los riesgos.

8. Desde su punto de vista, ¿cree que las políticas y marcos europeos y nacionales existentes agilizan y dinamizan el intercambio de información sobre amenazas terroristas? ¿Qué se podría hacer para catalizar esta tarea?

Sin duda. Los países han avanzado notablemente en lo referente al intercambio de información, en el reconocimiento de que el terrorismo es una amenaza global que debe ser tratada de forma multinacional y en relacionar la seguridad externa y la interior. De hecho, estamos colaborando activamente con nuestros vecinos europeos, mediterráneos, trasatlánticos y del este. Y desde 2004 la mayoría de los estados miembros tienen centros de coordinación – como podrían ser el caso del CITCO en España– para mejorar la cooperación a todos los niveles. Además, Europol pretende consolidarse como una plataforma multinacional visible y cuyas herramientas permitan mejorar las capacidades de investigación del terrorismo de los Estados Miembros.

4 Informes y análisis sobre ciberseguridad publicados en mayo de 2016

The Temptation of Technological Warfare….again (THIBER)



Digital Investment Data and Growth in Europe: A framework for analysis (ECIPE)

Qualified Website Authentication Certificates (ENISA)

Informe Anual de Seguridad Nacional 2015 (DSN – Gobierno de España)

2015 Internet Crime Report (FBI)

Mobility Report 2016 (Ericsson)

The Federal Big Data Research and Development Strategic Plan (White House)

Competition Law and Data (Bunderkartellamnt)

5 HERRAMIENTAS DEL ANALISTA: Mobile Security Framework (MobSF)

Mobile Security Framework (MobSF) es una plataforma inclusiva de inteligencia de código abierto para móviles (tanto Android como iOS) que permite automatizar un completo test de intrusión y análisis técnico de vulnerabilidades de apps, tanto estático como dinámico.

A través de una sencilla interfaz web, el usuario puede subir binarios de Android e iOS (ficheros APKs e IPAs respectivamente), realizando en el primero caso incluso un reversing del código fuente de la app, obteniendo el código fuente completo, análisis de permisos, certificados digitales, Manifest e info.plist, entre otros.

Del mismo modo, también puede ejecutar análisis dinámicos (sandboxing) de apps, llegando incluso a realizar pruebas de seguridad de la API Web con su API Fuzzer, permitiendo hacer recopilación de información, análisis de seguridad de cabeceras, identificar vulnerabilidades específicas de la API móvil como XXE (XML External Entity), SSRF (Server Side Request Forgery), path transversal, IDOR (Insecure Direct Object References), y otras cuestiones relacionadas con la sesión y la limitación de rate de la API.

Esta herramienta es de especial utilidad no sólo para analistas de seguridad sino también para aquellos desarrolladores interesados en incluir la seguridad en el ciclo de vida del desarrollo software.

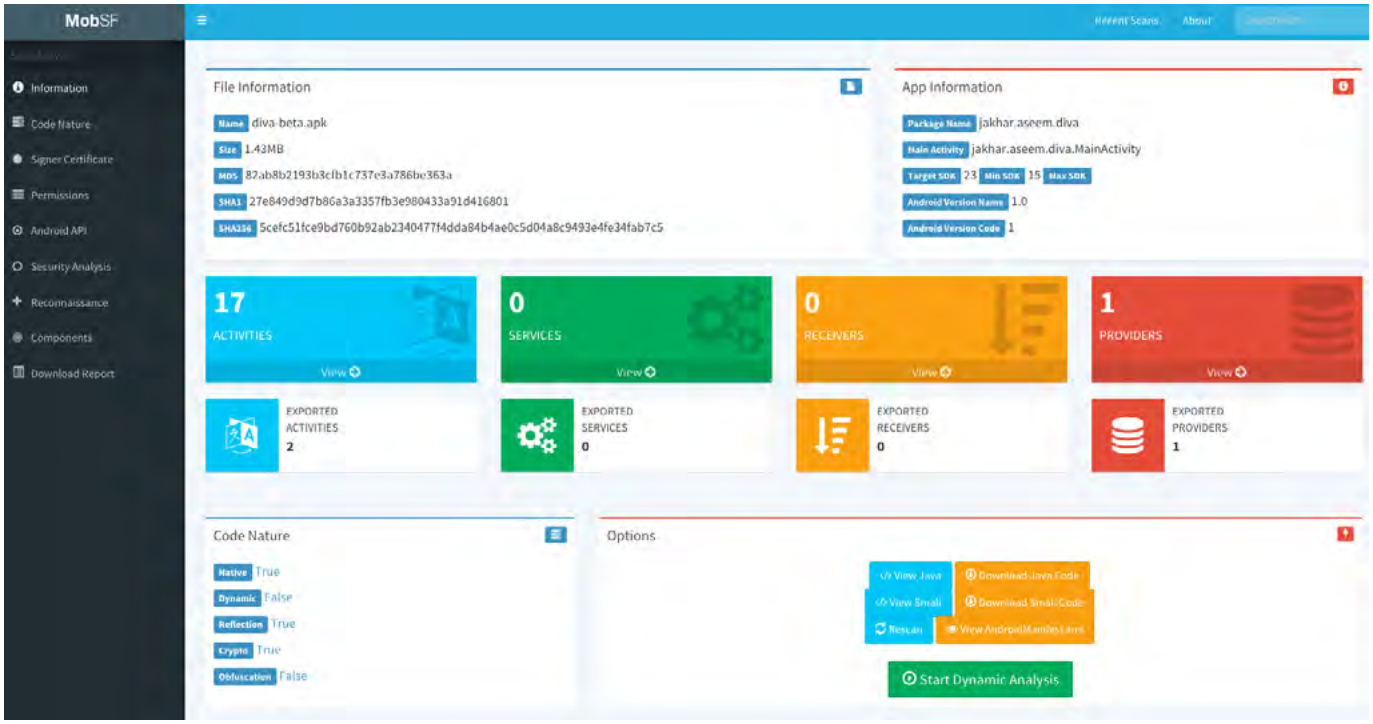


Ilustración 1 Ejemplo de análisis estático de una app Android (APK)

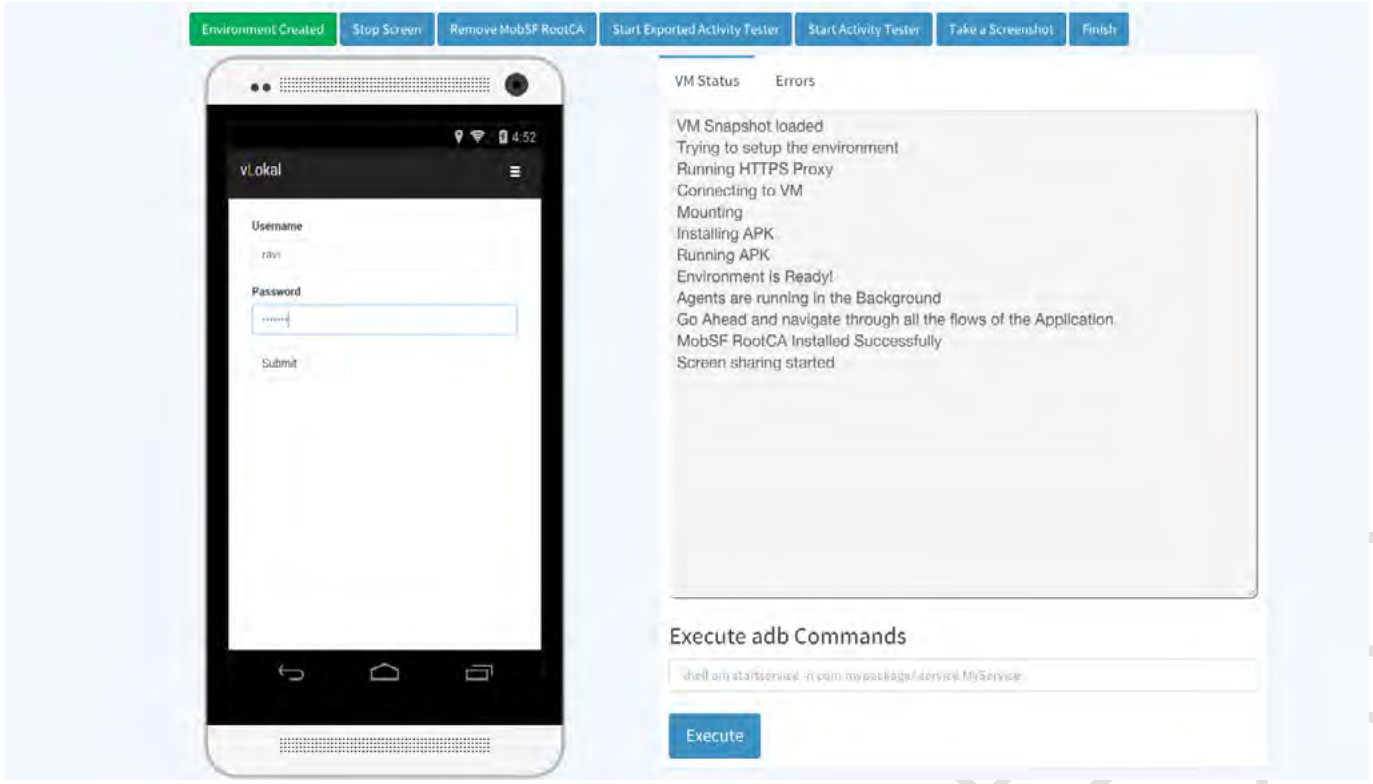


Ilustración 2 Análisis dinámico de una app Android (APK)

6 Análisis de los Ciberataques del mes de mayo de 2016

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

CIBERCRIMEN

A comienzos del mes de mayo, *se publicó un archivo de 10 GB conteniendo datos financieros sensibles de un banco en los Emiratos Árabes.* Basado en el análisis inicial del conjunto de datos filtrado, se determinó que los datos pertenecían a Investbank, basado en Sharjah, afectando a decenas de miles de sus clientes.

Los datos expuestos incluyen carpetas llamadas 'Account Master', 'Customer Master' y 'Branch Master', consistiendo principalmente en hojas de cálculo, archivos PDF e imágenes supuestamente filtrados desde una base de datos interna. Adicionalmente, existe un documento titulado 'Tarjetas', conteniendo cerca de 20.000 PANes, mientras que otros ficheros contienen más de 3.000 extractos de cuenta individuales, todos ellos con las marcas de agua y logotipos de Investbank.

Ilustración 1 captura de pantalla de una porción de los datos robados a Invest Bank

Otros archivos relevantes en la fuga de datos hacen referencia a 'inversores', 'documentos de tierras' y 'pasaportes'.

Según reconoce el propio banco, fueron víctimas de una extorsión a finales de 2015, mediante la cual un grupo autodenominado Bozkurtlar les reclamó el pago de 3 millones de dólares a fin de no publicar la información sustraída. Es por esto que los datos filtrados parecen no estar actualizados.

```
<%
    try {
    Class.forName("com.microsoft.jdbc.sqlserver.SQLServerDriver");
    } catch (ClassNotFoundException e) {
        out.println("<h1>Driver not found:" + e + e.getMessage() + "</h1>" );
    }
try {
    Connection conn = DriverManager.getConnection (
        "jdbc:microsoft:sqlserver://HOFWSPD02\\
        InvestBankAmbit:1303;user=sa;password=[redacted];databaseName=InvestBankAmbit;sendStringParametersAsUnicode=true",
    "sa", "invest98" );

        Statement stmt = conn.createStatement();
        ResultSet rs;

        rs = stmt.executeQuery("SELECT * FROM sys.servers");
    out.println( "<table>" );
        while ( rs.next() ) {
            String title = rs.getString("name");
            out.println("<tr><td>"+title+"</td></tr>" );
        }
    out.println( "</table>" );

        conn.close();
    } catch (Exception e) {
        out.println( "<h1>exception: "+e+e.getMessage()+"</h1>" );
    }
%>
```

Ilustración 2 Muestra del código empleado para acceder a la base de datos de Invest Bank

El pasado 17 de mayo se puso a la venta en diversos foros de la Deep web *una base de datos con más de 167 millones de credenciales* (identificador del usuario, email del usuario y hash sha1 del password) de usuarios de Linkedin. Aparentemente el origen de las credenciales se remonta a una filtración del año 2012, ya que ese mismo año se produjo *una fuga de credenciales afectando a más de 6,4 millones de usuarios.*

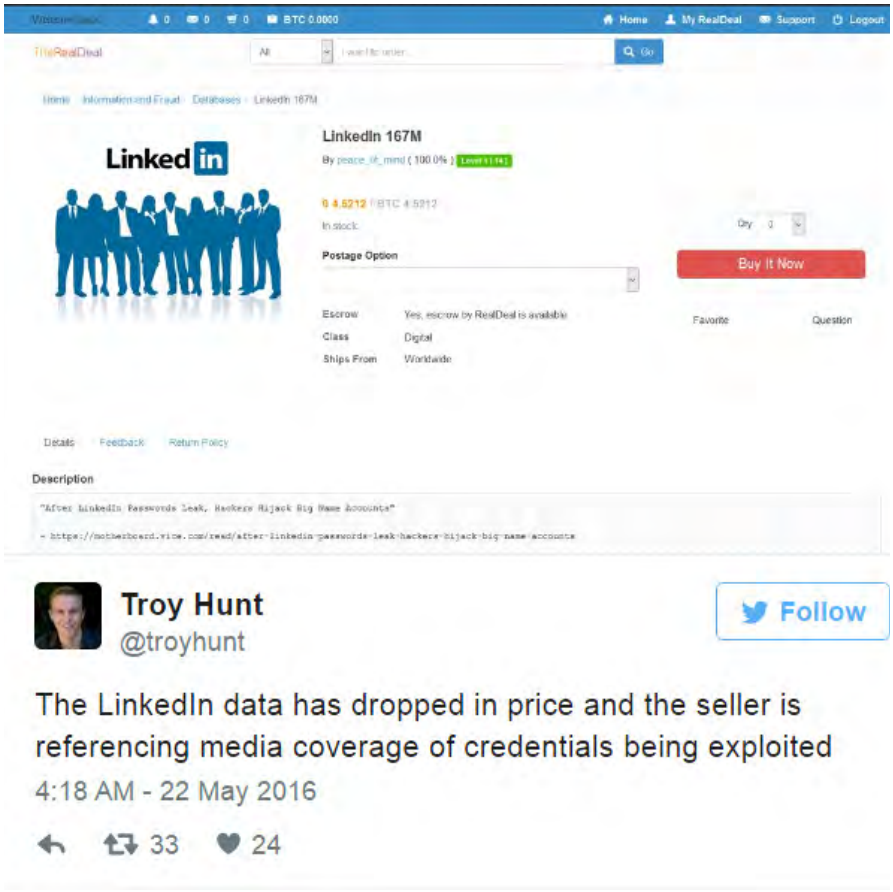


Ilustración 3 Venta del leak de usuarios de Linkedin por un precio inicial de 5 Bitcoins en un marketplace llamado TheRealDeal

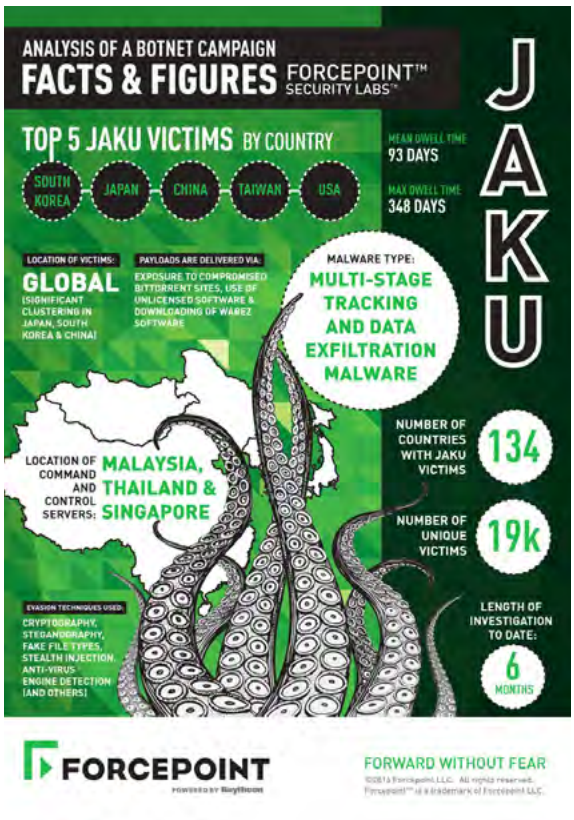
La compañía, siguiendo su política de gestión de crisis al efecto, ha procedido a reestablecer las credenciales de aquellos usuarios creados con anterioridad a 2012 y que no hubiesen cambiado su contraseña desde entonces. Al mismo tiempo, su departamento jurídico se ha puesto en contacto con los usuarios afectados para notificarles este acontecimiento.

Por otra parte *el mes pasado se produjo una filtración de datos de la Asociación Española de Desalación y Reutilización* a través de un ataque de inyección SQL en su web. Como consecuencia, se produjo una fuga de datos de los socios y empresas pertenecientes a la asociación. Entre la información afectada se encuentran credenciales corporativas de empleados asociados con este sector de actividad, así como DNI, teléfono, email y otros datos personales.

El presunto autor autodenominado Pyopzi según se mostraba en su perfil de Twitter, aparentemente ha estado relacionado con otras operaciones contra intereses de empresas de diversa índole bajo la operación #opBeast.

CIBERESPIONAJE

En el ámbito del ciberespionaje, a comienzos de mes se descubrió una botnet desconocida hasta la fecha, desarrollada específicamente para realizar un ataque faseado orientado a la exfiltración de datos, cuyos objetivos parecen estar focalizados en Asia.



Sus descubridores explican en *su informe de amenazas de 2016 que Jaku*, como se ha denominado a esta botnet, fue descubierto como resultado de una investigación de seis meses por el equipo de Investigaciones Especiales (SI) de Forcepoint, como se detalla en informe global de amenazas publicado por la compañía. Aparentemente se ha cobrado 19.000 víctimas en 134 países hasta el momento.

Jaku realiza infecciones masivas y lleva a cabo ataques a víctimas específicas posteriormente a través de la ejecución de las campañas operativas simultáneas muy concretas.

Forcepoint explica que las víctimas se encuentran en todo el mundo, pero hay agrupamientos significativos en Asia, especialmente en Japón, Corea del Sur y China. Los servidores de comando y control se encuentran en Malasia, Tailandia y Singapur.

La firma de seguridad Symantec ha hecho público a comienzos de mes las operaciones de un grupo descubierto en julio de 2015, después de que se detectasen algunos sitios web comprometidos entregando el malware Gofarer a través de ataques en la descarga de ficheros y vulnerabilidades en Flash, lo que, a su vez, instalaba una puerta trasera denominada Daserf. Los investigadores de Symantec también exponen que el grupo utiliza a veces campañas de spear- phishing entregando archivos adjuntos de correo electrónico, que, al abrirse, explotaban la vulnerabilidad CVE-2014-4114 Microsoft Office para instalar la puerta trasera mencionada (Daserf).

Hasta este punto, el grupo, que Symantec ha llamado Tick, seguía constantemente un patrón común en sus ataques que se observa en la mayoría de las campañas de espionaje cibernético atribuidas al mismo. Los investigadores encontraron evidencia de la actividad del grupo en diversos ataques llevados a cabo durante un periodo temporal de casi diez años.

Symatec asegura que Tick ha sido muy activo, centrando gran parte de sus esfuerzos en no ser detectados. El grupo parece estar focalizado en empresas japonesas y ha dirigido sus ataques por lo menos contra siete empresas de alta tecnología, ingeniería acuática, y sectores de broadcasting

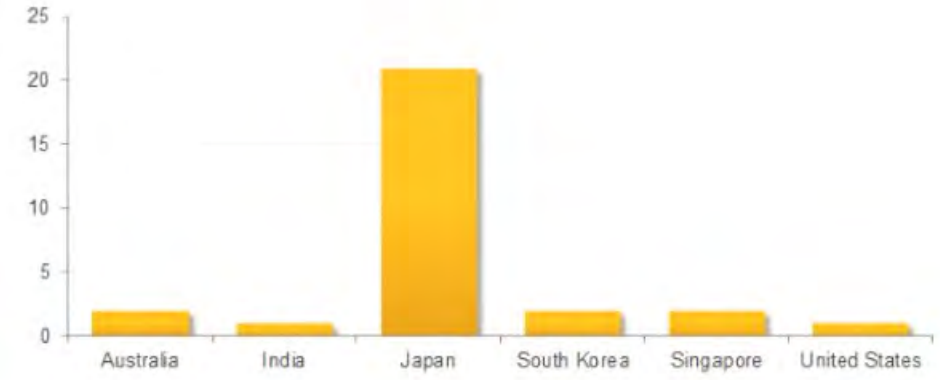


Ilustración 4 Objetivos de los ataques de Tick

HACKTIVISMO

En el ámbito del hacktivismo cabe destacar la intensa actividad nacional contra diversos organismos locales y nacionales de las fuerzas y cuerpos de seguridad del estado.

El 17 de mayo, un grupo de ciberactivistas actuaron contra los Mossos d'Esquadra, en concreto, contra el sindicato Sindicat dels Mossos d'Esquadra (SME). Decenas de datos personales de sus afiliados se filtraron en la red, y la web y la cuenta de Twitter sufrieron un defacement.

Durante más de ocho horas, *la cuenta en la red social del sindicato* estuvo publicando contenidos a favor de derechos humanos y en contra de las torturas. Además, cuando se accedía a su web corporativa, se podía leer un comunicado sobre una supuesta refundación del sindicato. "Hemos decidido dejar de hacer la faena sucia como soldados rasos del capitalismo".

También, a través de Twitter, divulgaron los datos personales de más de 5000 agentes relacionados con el sindicato, como teléfonos, direcciones de correo electrónico, direcciones postales e incluso cuentas corrientes.

Ilustración 5 La cuenta de twitter hackeada

Finalmente, el 31 de mayo, en una acción aparentemente realizada por parte del colectivo Anonymous (si bien su autoría y relación con el grupo original está actualmente en entredicho por su modus operandi), se han difundido los datos personales de 5.400 policías nacionales en protesta por la "Ley Mordaza".

La acción ha sido reivindicada por un grupo que asegura pertenecer al colectivo Anonymous. La cuenta de Twitter *@FkPoliceAnonOps*, asociada a los autores de la filtración, ha publicado diversos enlaces en los que se puede acceder a todos los datos filtrados.

La filtración se ha producido tras el ataque a la web *mupol.es*, de la mutua de la Policía Nacional, Mutualidad de Previsión Social de la Policía. La página que estuvo offline varios días, actualmente muestra un mensaje explicando lo ocurrido.

La publicación *de los datos de los 5.400 funcionarios* y agentes incluye sus contraseñas de acceso (hashes) a sus credenciales en la página mupol.es, además de sus nombres completos, correos electrónicos y DNIs. De momento se desconoce si todos los datos filtrados están actualizados y en pleno funcionamiento, aunque como suele ocurrir en estas ocasiones es probable que una parte se trate de emails y contraseñas en desuso. Aun así, se trata de una filtración grave que llega pocos días después del ataque a la página web del sindicato de los Mossos d'Esquadra SME.

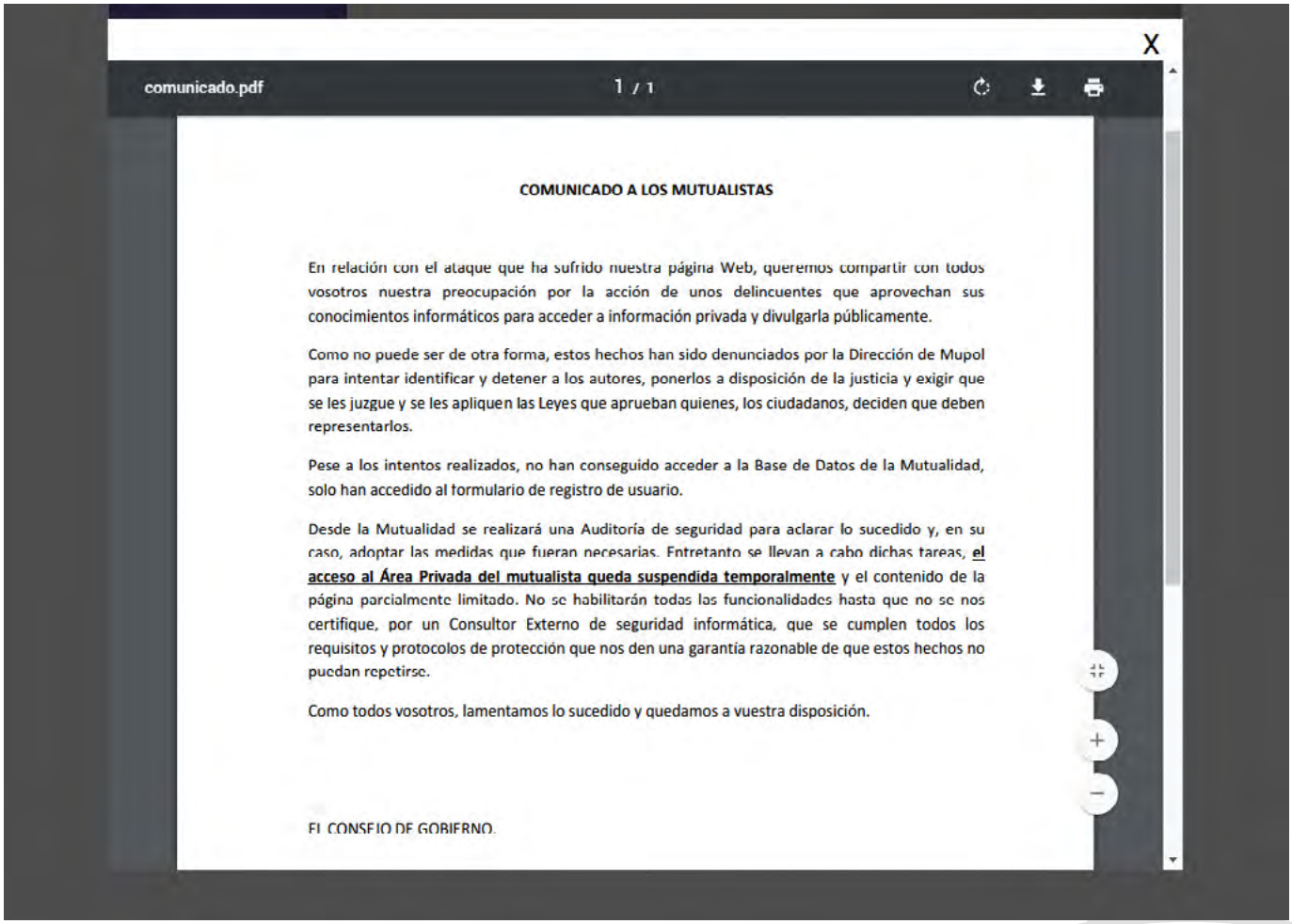


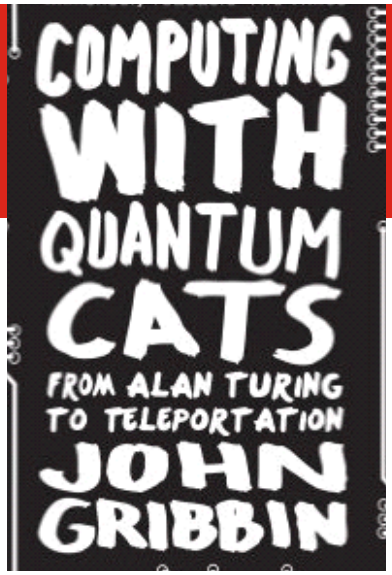
Ilustración 6 Mensaje en la web de Mupol

7 Recomendaciones

7.1 Libros y películas

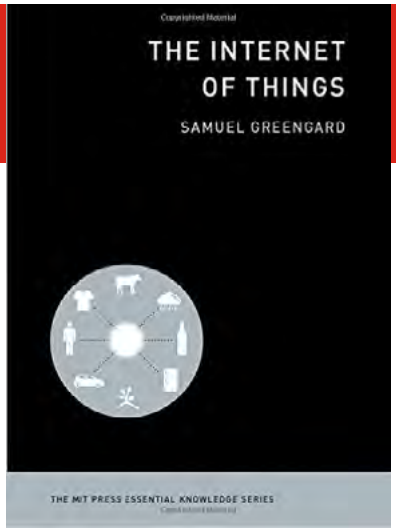
Película:
ESPÍAS DESDE EL CIELO

Sinopsis: La coronel Katherine Powell (Helen Mirren), una oficial de la inteligencia militar británica, lidera una operación secreta para capturar a un grupo de terroristas en Nairobi, Kenia. Cuando se da cuenta que los terroristas están en una misión suicida, ella debe cambiar sus planes de 'capturar' por 'matar'. El piloto estadounidense de drones Steve Watts (Aaron Paul) recibe la orden de destruir el refugio donde se hallan los terroristas, pero una niña de nueve años ingresa en la zona donde podría ser herida. Posiblemente una de las mejores películas que describen la guerra moderna y la inteligencia mediante el uso de drones.



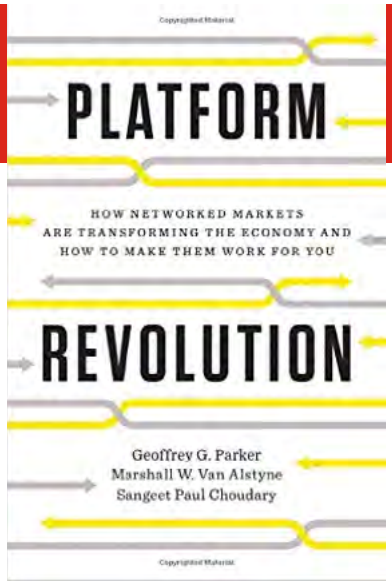
Libro:
COMPUTING WITH QUANTUM CATS: FROM COLOSSUS TO QUBITS

Autor: John Cribbin
Num. Paginas: 304
Editorial: Black Swan
Año: 2015
Precio: 15.95 Euros
Sinopsis: John Cribbin hace un preciso análisis de como la Tecnología cuántica ha pasado de la ciencia ficción a hacerse realidad; analizando como las comunicaciones serán cada vez más rápidas y como el tele-transporte podría dejar de ser una quimera.



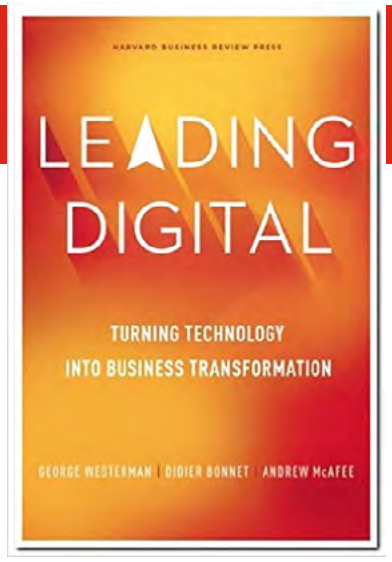
Libro:
THE INTERNET OF THINGS

Autor: Samuel Greengard
Num. Paginas: 184
Editorial: MIT Press
Año: 2015
Precio: 11.00 Euros
Sinopsis: Samuel Greengard nos ofrece una visión tecnológica del Internet de las Cosas (IoT) y como cambiará el mundo. Greengard describe lo que será un día cualquiera de 2025 en el que personas, dispositivos y objetos vivirán en un mundo hiperconectado.



Libro:
PLATFORM REVOLUTION

Autor: Geoffrey G.Parker, Marshall Van Alstyne y Sangeet Choudary
Num. Paginas: 384
Editorial: WW Norton and Co.
Año: 2016
Precio: 20.00 Euros
Sinopsis: Los autores ofrecen una visión exhaustiva de un nuevo modelo de negocio: las plataformas. Basándose en el análisis de plataformas como Uber, Facebook o Alibaba, se proponen las líneas maestras para la creación de un mercado de plataformas.



Libro:
LEADING DIGITAL

Autor: George Westerman, Didier Bonnet y Andrew McAfee
Num. Paginas: 256
Editorial: Harvard Business Review Press
Año: 2014
Precio: 25.00 Euros
Sinopsis: Los autores proporcionan una guía imprescindible que ayudará a las organizaciones a sobrevivir y prosperar en el nuevo y potente mercado digital.

7.2 Webs recomendadas

https://www.cesg.gov.uk/
Sitio web de la Autoridad Nacional para la Seguridad de la Información del Gobierno Británico.

http://unaaldia.hispasec.com/
Sin duda, "Una al día" es uno de los servicios más relevantes de noticias y análisis sobre ciberseguridad en español.

http://www.thecyberwire.com/
Cyberwire es un sitio web que proporciona análisis propios de las noticias más relevantes que acontecen en el ciberespacio.

http://www.recode.net/
Recode es un sitio web especializado en el análisis de noticias tecnológicas en la que los principales expertos mundiales aportan su visión sobre la materia.

http://www.cbronline.com/
Sitio web especializado en el análisis de noticias relacionadas con el Big data y el IoT.

http://www.ted.com/
Sitio web de TED, donde se pueden encontrar interesantes conferencias sobre el mundo de las nuevas tecnologías.

7.3 Cuentas de Twitter

@david_barrancos

@Cyberchallenge

@cyberstreetwise

@Recode

@sbarrera0

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
2-3 junio	Fort Meade, Maryland, United States	NSA	NSA SIGINT Development Conference 2015	https://www.fbcinc.com/event.aspx/Q6UJ9A010V27
7-8 junio	Bratislava, Slovakia	BACEE	Hacking Financial Institutions	http://ictsecurityconference.eu/
7 de junio	Londres	Infosecurity Group	Infosecurity Europe	http://www.infosecurityeurope.com/
7 de junio	Madrid	Check Point	Cyber Day 2016	https://www.checkpointiberia.es/cyber-day-2016/cyber-day-2016.html
8-9 junio	Madrid	ISACA	High Level Conference on Assurance	http://www.isaca.org/chapters7/madrid/events/eventos/pages/high-level-conference.aspx
11-12 junio	São Paulo, Brazil	B Sides	BSides Latin America Edition Brazil	http://www.securitybsides.com/w/page/104120015/BSidesLatam
12- 17 junio	Seul, Korea	FIRST	FIRST Conference	https://www.first.org/conference/2016
14 de junio	Madrid	Red Seguridad' y 'Seguritecnia'	VIII Encuentro de la Seguridad Integral (Seg2)	http://www.redseguridad.com/eventos/agenda-del-sector/viii-encuentro-de-la-seguridad-integral-seg2
15-17 junio	Granada	INCIBE	II Jornadas de Investigación en Ciberseguridad	http://ucys.ugr.es/jnic2016/
16 - 17 junio	Lisboa, Portugal	ISEG, University of Lisbon	2016 European Security Conference	http://secconf.iseg.ulisboa.pt/
18 junio	San Sebastian, España	Asociación de Seguridad Informática EuskalHack	EuskalHack 2016	http://www.euskalhack.org/index.php/es/
19 - 22 Junio	Chengdu, China	IEEE	IEEE Cyber 2016	http://www.ieee-cyber.org/2016/
27 junio - 2 julio	Roma, Italia	OWASP	AppSec Europe MMXVI	https://2016.appsec.eu/

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

www.thiber.org
twitter.com/thiber_esp
www.linkedin.com/groups/7404269