OCTUBRE 2015 / Nº 7

CIBER elcano

Desarrollado por:

INFORME MENSUAL DE CIBERSEGURIDAD

Copyright y derechos:

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

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

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

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

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

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank

Índice

1 Comentario Ciberelcano 04

2 Análisis de actualidad internacional 06

3 Opinión ciberelcano.....12

4 Entrevista a Miguel Rego 15

5 Informes y análisis sobre ciberseguridad publicados en septiembre de 2015... 20

6 Herramientas del analista 21

7 Análisis de los ciberataques del mes de septiembre de 2015 23

8 Recomendaciones

8.1 Libros y películas 31

8.2 Webs recomendadas 33

8.3 Cuentas de Twitter.....33

9 Eventos.....34

1 COMENTARIO CIBERELCANO:
¿Diplomacia para luchar contra el ciberespionaje?

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

Xi Jinping y Barack Obama en una rueda de prensa conjunta en la Casa Blanca. Foto: *© REUTERS/Gary Cameron.*

La **seguridad y defensa del ciberespacio** siguen ocupando un lugar prioritario en las agendas políticas de Washington y Beijing, tal y como se demostró la semana pasada durante la *visita oficial* del presidente chino **Xi Jinping** a los Estados Unidos.

La firme intención de la administración Obama –presionada por los gigantes tecnológicos del país- de aplicar importantes sanciones económicas a aquellas entidades chinas –públicas y privadas- relacionadas con las **campañas de ciberespionaje** contra empresas estadounidenses condicionó la preparación de la visita de la delegación china.

Recordemos que el pasado 1 de Abril, tan solo unos meses después de que Washington impusiese importantes sanciones económicas al régimen de Pyongyang como consecuencia del ciberataque sufrido por la compañía Sony, el presidente Obama firmaba una *Orden Ejecutiva* por la que autoriza al secretario de Hacienda –en coordinación con el fiscal general de Estado y el secretario de Estado– a sancionar a aquellos actores extranjeros cuyas actividades en el ciberespacio supongan una amenaza para la seguridad nacional, la política exterior o la estabilidad económica y financiera del país.

A pesar de las reticencias de Washington y de las presiones de la industria estadounidense, ambos gobiernos se proponen dar una oportunidad a la **vía diplomática** para resolver el sempiterno problema del ciberespionaje. En este sentido, ambos gobiernos han acordado:

· **Intercambiar información sobre investigaciones relacionadas con actividades maliciosas en el ciberespacio**. Sin embargo, parece poco probable que EEUU y China puedan acordar una definición común sobre los límites de una 'actividad maliciosa en el ciberespacio'. Además, resultara aún menos probable que ambos gobiernos intercambien información relacionadas con sus áreas de investigación, máxime cuando estas son fundamentales para mantener su condición de potencia cibernética.

· **No apoyar actividades de ciberespionaje que puedan menoscabar los intereses comerciales e industriales de ambos países.** "Perseguir" con todos los medios humanos, legales y técnicos a su alcance las actividades de ciberespionaje que sean llevadas a cabo desde sus territorios nacionales hubiese sido la fórmula más adecuada para cimentar la lucha de ambos países contra el ciberespionaje.

· **Identificar y promover normas de buena conducta en el uso del ciberespacio por parte de los Estados.** Ambas delegaciones han reconocido la importancia del trabajo de las Naciones Unidas, a través de un grupo de experto gubernamentales, sobre las normas para un uso apropiado del ciberespacio por parte de los gobiernos. Sin embargo, este hecho contrasta con la propuesta de *gobernanza global del ciberespacio* abanderada por **Rusia y China** –rechazada por EEUU y la inmensa mayoría de la comunidad internacional- en la cual se otorga a cada Estado la legitimidad necesaria para controlar todo lo concerniente a sus ciberespacios específicos.

En definitiva, el **ciberespionaje** es un problema al que se enfrentan buena parte de los ciudadanos, la mayoría de las empresas y casi la totalidad de los gobiernos, cuya solución requerirá algo más que un lenguaje ambiguo y un acuerdo de mínimos desde la vía diplomática..

"parece poco probable que EEUU y China puedan acordar una definición común sobre los límites de una 'actividad maliciosa en el ciberespacio"

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

No sé lo que pasa en mi red. ¿Puedo protegerla adecuadamente?

AUTORES: Dr. José Ramón Coz Fernández. Analista Internacional de THIBER. Investigador en la Universidad Complutense de Madrid.

Vicente José Pastor Perez. Jefe de los Servicios de Seguridad Empresarial en la Agencia de Comunicaciones e Información de la OTAN

INTRODUCCIÓN

A pesar de todo el camino recorrido ya hacia mayores niveles de gobierno en la gestión de los servicios y las tecnologías de la información, no es inusual encontrar en las grandes empresas y organizaciones que los silos que separan unas actividades de las otras impiden una correcta coordinación de esfuerzos. Esto se traduce en un conocimiento imperfecto de la situación de nuestras redes y sistemas en todo momento y la protección y defensa de éstos depende en gran medida de esta información. De otro modo, es muy probable que todas nuestras defensas se enfoquen en algún lugar de nuestros sistemas mientras que existen otros que no sólo no están protegidos adecuadamente sino que además no somos conscientes de ello.

Hablar de la tendencia a utilizar Cyber Threat Intelligence, sin ser capaces de "interrogar" a nuestros sistemas respecto a esos Indicadores de Compromiso, no resolverá el problema para ser capaces de encontrar si estamos o no afectados por las amenazas continuas en nuestro entorno.

Es el Arte de la Guerra Sun Tzu: ¿Qué pasa si no te conoces a ti mismo? Que no se puede defender lo que no se conoce.

Este artículo pretende mostrar las dificultades que se presentan para ejercer una ciberdefensa eficaz el hecho de que los procesos, las tecnologías y los equipos humanos que se dedican a la gestión de los sistemas de información y los que se dedican a defenderlos de ataques externos, estén separados unos de otros.

DESCONEXIÓN ENTRE EL SOC Y EL NOC. ¿NO LA RESOLVIÓ EL NSOC?

Hace ya varios años que se propuso la unión de los Centros de Operaciones de Seguridad *(Security Control Centres – SOCs)* y los Centros de Operaciones de Red *(Network Control Centres – NOCs)* en un único Centro de Operaciones de Red y de Seguridad *(Network and Security Operations Centre – NSOC)*. Sin embargo algunas organizaciones realizaron únicamente una unión en la localización física y no armonizaron los procesos que debían utilizar.

La implementación de Sistemas para la Gestión de Servicios de Tecnologías de la Información *(Information Technology Service Management - ITSM)* junto con Sistemas de Gestión de la Seguridad de la Información *(Information Security Management System – ISMS)* basándose en estándares internacionales tales como ISO/IEC 20000 e ISO/IEC 27001,

además de sistemas de buenas prácticas tales como ITIL *(Information Technology Infrastructure Library* – Biblioteca para las infraestructuras de tecnologías de la información), así como controles de gobierno como los que se describen en COBIT (Control Objectives for Information and Related Technology), o las buenas prácticas para la gestión de los proyectos y programas como PRINCE 2 o MSP (Managing Sucessful Programs) es altamente complicada.

Hay que, en primer lugar, asumir la realidad de que la implantación de unas normativas y unos procesos del nivel de madurez que reclaman estos estándares y buenas prácticas no es, ni mucho menos, gratis, ni rápida ni sencilla, y que su retorno de inversión suele ser complejo de evaluar. Más si cabe en el caso de llevar a integrar todos ellos de forma armonizada y cuando están en unos entornos que tienen de por sí unas normativas y procedimientos de seguridad muy estrictos y poco flexibles, y están sometidos a unas amenazas cada vez más y más sofisticadas.

Incluso en las organizaciones y grandes corporaciones donde el grado de inversión en Tecnologías de la Información y Comunicaciones es de decenas, centenas o incluso miles de millones de euros, como pueda ser el caso de la OTAN, y donde el grado de inversión en Ciberseguridad es proporcionalmente más adecuado, este problema se antoja muy complejo de resolver.

Imagen 1: Vista de la Sede Central de la OTAN en Bruselas. (Fuente: Biblioteca multimedia de la OTAN, Septiembre 2015). El grado de Inversión de OTAN manejado por la Agencia de Comunicaciones e Información es de miles de millones de euros.

Un aspecto capital en este punto es la balanza de inversiones entre procesos, recursos humanos y equipamiento. Si no se logra un equilibrio razonable en este punto, la balanza se romperá por el lado más débil. Pese a que nuestras organizaciones tengan una razonable integración entre los SOC y los NOC, e incluso para aquellas entidades que dispongan de NSOC lo suficientemente maduros, si esta balanza no está correctamente equilibrada las amenazas se verán materializadas.

Pero es que, aun así, nos quedaría otra batalla que ganar y es la integración entre el, supuestamente maduro, NSOC con el resto de los procesos de negocio.

EL NSOC NO ESTÁ CONECTADO CON EL RESTO DE LOS PROCESOS DE GESTIÓN

Como ya hemos mencionado con anterioridad ya es de por sí un reto la integración entre los Centros de Operaciones de Seguridad y los Centros de Operaciones de Red, pero es que aunque dispusiéramos de un centro único totalmente integrado con un conocimiento global de la situación de nuestra corporación a nivel detallado, incluyendo no solamente una visión global de la seguridad a nivel de red, servidores y clientes finales, sino también una visión coordinada de la administración a nivel de sistemas, si no integramos los procesos y los recursos humanos de soporte con el resto de procesos de negocio, será muy difícil de garantizar un nivel de riesgo aceptable.

¿Qué ocurre con la Gestión de los Cambios Tecnológicos y de Gestión de Sistemas? ¿Qué ocurre con la Gestión de los Proyectos y Programas que están en ejecución y modifican o van a modificar a futuro nuestras arquitecturas tecnológicas? ¿Qué ocurre con la gestión de la obsolescencia? ¿Qué ocurre con la Gestión de los Recursos Humanos de Soporte a los procedimientos de Gestión Tecnológica? ¿Y la Gestión Financiera? Estos aspectos, en muchos casos, son capitales y deben integrarse de la forma más adecuada en estos centros de soporte.

Si no hay una conexión entre los cambios que se producen, por muy bien que conozca mi entorno, será muy difícil mantener en el tiempo ese conocimiento. Y para ello hay que establecer unos vínculos muy estrechos y rigurosos con la gestión de proyectos y programas, con los cambios requeridos desde la propia explotación de los sistemas y con la gestión de la obsolescencia de equipamiento y sistemas.

Al fin y al cabo, todos los sistemas y las comunicaciones tienen un ciclo de vida que debe monitorizarse y que en muchos casos son muy cortos en el tiempo. Pensemos, por ejemplo, en el proceso necesario que permite, en organizaciones maduras, una integración entre la gestión de parches y el análisis de vulnerabilidades.

Imagen 2: Centro de Respuesta a Incidentes de Seguridad de la OTAN (NCIRC) durante una jornada de trabajo (Fuente: OTAN)

Otro aspecto fundamental es la gestión financiera. Si seguimos financiando proyectos con una balanza de costes muy acentuada en su desarrollo y muy baja en su mantenimiento, seguiremos cometiendo el error histórico de las inversiones tecnológicas y nos quedará muy poco margen para que los NSOC puedan adaptarse a las nuevas inversiones, quedándose cada vez como un elemento más y más marginal y perdiendo su función cable de soporte al negocio.

EL FACTOR CLAVE PARA LA SEGURIDAD: LOS RECURSOS HUMANOS

¿Qué ocurre con los recursos humanos? Evidentemente es el Core de la protección en la seguridad de cualquier entidad. Después de participar en numerosas mesas redondas, charlas, conferencias y estudios siempre hemos llegado a la misma conclusión: se habla mucho de tecnología, de sistemas, y poco de los recursos humanos que son el factor clave de la seguridad a nivel global, en cualquier organización, sea de la naturaleza que sea.

Imagen 3: La demanda de técnicos especializados en ciberseguridad es mucho mayor a la oferta actual disponible en el mercado Expertos trabajando en el sector de la Ciberseguridad. (Fuente: Biblioteca multimedia de la OTAN).

Y es que la integración entre los Centros de Seguridad y Operación de Red se comienza desde la integración del personal y su propia gestión. Por mucho que hayamos alcanzado de un grado de madurez elevado en Ciberseguridad y Protección de red y dispongamos de los mejores analistas forenses, de expertos en Gestión de Malware, equipos muy especializados en gestión de ciber-incidentes, en análisis de vulnerabilidades, en cifrado, en protección perimetral, en comunicaciones seguras, en gestión de claves y accesos, analistas de eventos y procesos de seguridad, etc. si no tenemos buenos arquitectos de sistemas, analistas de red, buenos equipos de soporte a las comunicaciones y a la gestión básica de incidencias, a la gestión de configuración o administradores de sistemas que conozcan las reglas de negocio aplicadas a nivel de cada sistema, será muy difícil lograr la visión conjunta que se precisa.

Aquí nos enfrentamos, además, a otra problemática compleja: la gestión de la externalización. En el mundo de la tecnología y las comunicaciones la externalización es la tónica, y saber que tengo, debo o puedo externalizar es un aspecto muy poco claro, sobretodo en entornos poco maduros tecnológicamente. Pero es que en Ciberseguridad todavía está mucho menos claro, al tener la mayor parte de las organizaciones, aún, una madurez muy baja en este campo y, además, en un entorno donde la demanda de especialistas supera a la oferta.

¿Qué procesos debo externalizar: la gestión de Ciberincidentes, el análisis forense, la administración de sistemas, la arquitectura corporativa, la gestión de configuración? ¿Cuáles son los perfiles más adecuados para cada uno de ellos? ¿Un analista de eventos de seguridad tiene el mismo perfil que un administrador de sistemas?

Además, siempre hay que tener muy presente que externalizar requiere monitorizar la externalización y eso suele añadir una capa extra en la organización. Externalizar no significa que la responsabilidad quede delegado en un tercero ni tampoco que el coste del servicio se transfiera totalmente a la entidad externalizada.

Por ultimo está otro aspecto clave: la segregación de funciones. ¿El analista forense puede ser un administrador de sistemas? ¿Debo externalizar la función de auditoria de sistemas y no la de gestión de cambios? ¿Los propios operadores de red pueden gestionar las incidencias tic? ¿Y los Ciberincidentes? ¿Puedo tener los mismos roles para ambas incidencias? ¿La misma entidad que explota mis sistemas debe ser la que me ofrezca el servicio de continuidad de negocio?

Todos estos asuntos hay que tenerlos muy claros y solo desde una adecuada gestión de recursos humanos y de contratación se podrán resolver estas problemáticas.

Imagen 4: Los autores en el Centro de Operaciones del Centro de Respuesta a Incidentes de Seguridad de la OTAN

¿CÓMO LO SOLUCIONAMOS?

No hay una única solución o receta mágica, pero sí que existen unos ingredientes que se antojan casi obligatorios:

- Adecuación a los estándares más al uso y adaptación organizacional a un coste razonable y siempre dentro de las políticas, normativas y procedimientos de seguridad de la información corporativos.

- Integración necesaria entre los Centros de Seguridad y Operaciones de Red. Esto incluye una gestión común del personal.

- Coordinación a nivel de procesos de soporte a la seguridad y las operaciones y los procesos clave de negocio, incluyendo la gestión financiera, de recursos humanos, del cambio tecnológico y de la gestión de proyectos y programas.

- Considerar a los recursos humanos como el factor clave en la protección organizacional y crear políticas que permitan una gestión normalizada de los recursos de soporte a los centros de explotación y seguridad de la información.

- Gestión adecuada de la externalización y monitorización de los servicios externalizados.

- Una segregación de funciones razonable, equitativa y analizada que permita asumir riesgos razonables de control.

Por supuesto, existen muchos otros ingredientes importantes, pero queremos destacar algunos de los que hemos considerado más críticos para resolver las problemáticas planteadas.

RESUMEN

En el presente artículo hemos expuesto la problemática compleja de la protección de la información a nivel organizacional. Hemos cubierto varios aspectos de esta problemática que consideramos esenciales, como la integración entre los Centros de Operaciones de Seguridad y los Centros de Operaciones de Red, la adaptación a diversos estándares internacionales y buenas prácticas, la integración de los Centros Integrados con los procesos de negocio, y hemos analizado una serie de aspectos de importancia capital como la gestión de los recursos humanos, la externalización de servicios y la segregación de funciones.

Finalmente, hemos incluido una serie de ingredientes que consideramos clave a la hora afrontar una gestión global razonable de la seguridad de la información y la protección de nuestras organizaciones.

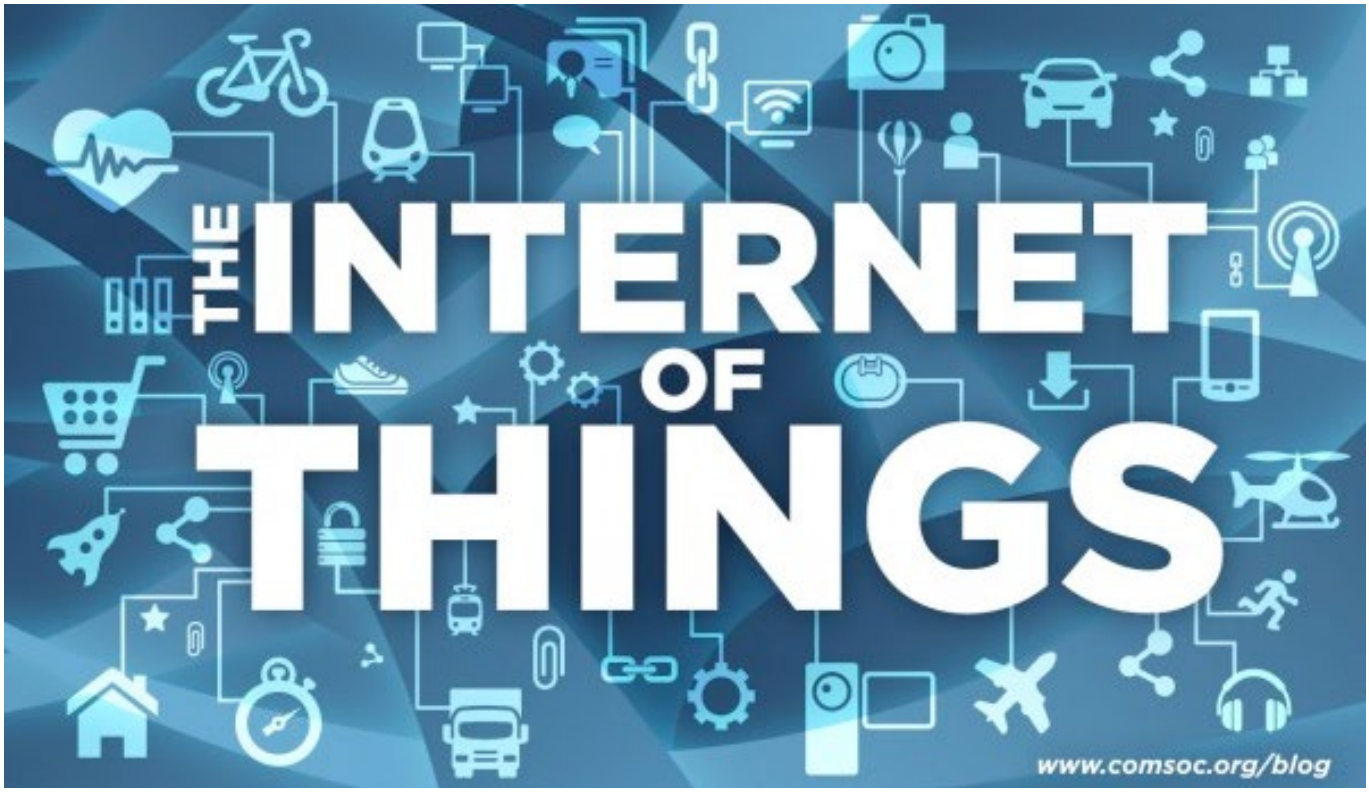
3 OPINIÓN CIBERELCANO
El 'Internet militar de las Cosas'

AUTOR: Guillem Colom. Director de THIBER, the cybersecurity think tank.

Aunque las experiencias recientes podrían sugerir que la integración y explotación de la cibernética en el ámbito militar es algo nuevo, lo cierto es que sus orígenes se sitúan en la década de 1960; y los primeros intentos de integrar en red las plataformas, sensores y armas datan de los años setenta. Hoy en día, la cibernética no sólo se ha consolidado como una dimensión fundamental del planeamiento y conducción de las operaciones militares, sino que todos los sistemas, armas, plataformas y procesos se fundamentan en el poder de la red para realizar sus funciones.

De hecho, podríamos afirmar que existe un "Internet militar de las Cosas" que integra todos aquellos dispositivos que, conectados en red, proporcionan información sobre el funcionamiento, mantenimiento y seguridad de los sistemas de Mando y Control, aviones, barcos, carros de combate, misiles, proyectiles inteligentes, robots, drones, satélites o sistemas personales.

Ha pasado más de medio siglo desde que la *Agencia de Proyectos de Investigación Avanzados de Defensa* (DARPA) del Pentágono estadounidense concibiera el proyecto ARPANET – precursor de Internet – para crear una red de comunicaciones capaz de sobrevivir a una caída de los sistemas tradicionales por causas naturales o por un ataque nuclear. Desde entonces, esta red de redes se ha integrado progresivamente en los ejércitos hasta convertirse en un elemento esencial para su funcionamiento, administración, gestión u operaciones.



Aunque las Tecnologías de la Información y las Comunicaciones (TIC) se han integrado en las fuerzas armadas para mejorar su gestión y funcionamiento, su mayor beneficio ha sido lograr una capacidad sin precedentes para obtener, procesar, filtrar e interpretar ingentes volúmenes de información de interés militar; compartirla a todos los usuarios que la puedan necesitar de manera casi instantánea y neutralizar cualquier amenaza con una rapidez, precisión y eficacia sin precedentes y sin la necesidad de exponer innecesariamente las fuerzas propias al fuego enemigo.

No obstante, a pesar de que las TIC, la robótica o la inteligencia artificial se han integrado en nuevas plataformas (furtivas y no-tripuladas); sensores (Mando, Control, Comunicaciones y Computación e Inteligencia, Vigilancia, Adquisición de Objetivos y Reconocimiento) y armas (de precisión e inteligentes) para proporcionar importantes mejoras en la forma de concebir, plantear y conducir las operaciones; lo realmente relevante es que este conjunto de sistemas puedan trabajar en red, permitiendo que cualquier soldado sea capaz de conocer y controlar todo lo que sucede a su alrededor, bien sea reconociendo el terreno, identificando las amenazas, designando los objetivos o atacando los blancos en función de su situación, riesgo o disponibilidad.

Ésta es la premisa sobre la que se fundamenta el **sistema de sistemas**, basado en la capacidad de la integración en red de todos los elementos de las fuerzas armadas para acumular una inmensa cantidad de información sobre el área de operaciones, convertirla en inteligencia útil para las fuerzas que operan sobre el terreno y aprovecharla de inmediato para derrotar al adversario. Éste, a su vez, ha sentado las bases de la **guerra en red** *(Network-Centric Warfare)*, basada en las posibilidades que brinda el sistema de sistemas para crear un nuevo estilo de combatir que, organizado en torno a pequeñas fuerzas conjuntas, integradas en red, organizadas en enjambres y distribuidas

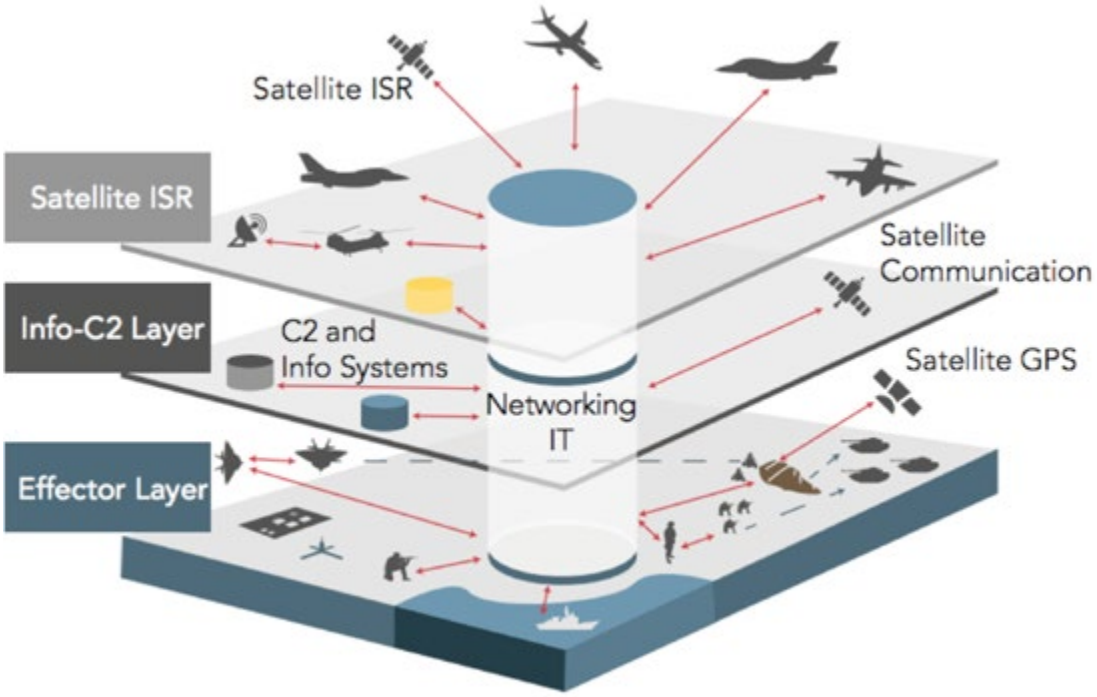


Figure 1: Network-centric warfare

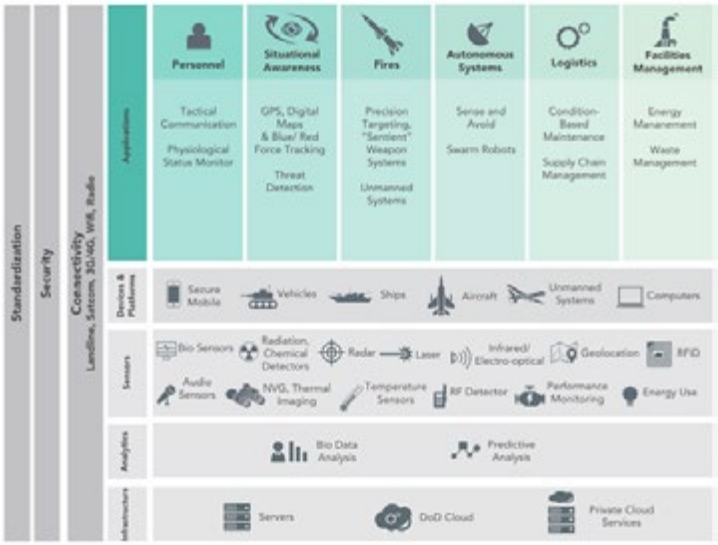
geográficamente por el campo de batalla, permita operar con una coordinación, flexibilidad, rapidez, precisión y seguridad sin precedentes en la historia, pudiendo identificar, fijar y batir los objetivos enemigos antes de que éstos se percaten de que han sido descubiertos. Aunque hoy en día la guerra en red contempla el empleo de humanos y sistemas informatizados, Estados Unidos pretende que en el campo de batalla futuro los robots – integrados todos en red y que requerirán ingentes volúmenes de información para funcionar – vayan sustituyendo progresivamente a los humanos.

"Estados Unidos pretende que en el campo de batalla futuro los robots vayan sustituyendo progresivamente a los humanos"

En consecuencia, la integración de sensores, decisores, plataformas, armas, tropas e infraestructuras en este meta-sistema cuya columna vertebral es la red no sólo optimiza el planeamiento y la conducción de las operaciones militares; sino también es uno de los pilares de los procesos de **transformación militar** de muchos países de nuestro entorno, de la Alianza Atlántica y, en cierta medida, de nuestro país.

No cabe duda de que el "Internet militar de las cosas" adquirirá una nueva dimensión a medida que se consoliden las tecnologías en materia de computación, *big data*, robótica, inteligencia artificial, *wearables* o integración de sistemas.

Exhibit 5. Military Tech Stack



4 Entrevista a Miguel Rego.
Director General del Instituto Español de Ciberseguridad (INCIBE)

1. Como Director General del Instituto Nacional de Ciberseguridad (INCIBE), ¿podría indicarnos cuáles son las principales competencias de la entidad? ¿Cuál es su rol en la implementación de la Estrategia de Ciberseguridad Nacional?

La actividad de INCIBE está basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, un hecho que se pone especialmente de manifiesto con nuestro Centro de Respuesta a Incidentes de Seguridad e Industria, el CERTSI, operado por personal de la entidad y coordinado conjuntamente por INCIBE y el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Este CERT Público Nacional que da soporte a ciudadanos, sector privado y empresas estratégicas, ha gestionado hasta el 31 de agosto de este año 37.000 incidentes de ciberseguridad. También es importante destacar el papel relevante que juega INCIBE en el desarrollo de la Estrategia Nacional de Ciberseguridad que se concreta en su capacidad de respuesta ante incidentes pero, también, por desarrollar proyectos e iniciativas para apoyar a las empresas españolas en el desarrollo del mercado nacional y en proyectos de internacionalización. Cabe destacar, igualmente, el "Programa de Excelencia en Ciberseguridad" que INCIBE está desarrollando para estimular, gestionar y retener el talento profesional en Ciberseguridad.

2. Para el desarrollo de esas actividades, ¿se cuenta con medios técnicos y personales propios o también con colaboración de la industria privada?

INCIBE recibe su financiación con cargo a los Presupuestos Generales del Estado y desarrolla servicios 100% públicos que proporciona sin contraprestación económica. INCIBE cuenta con alrededor de 90 empleados pero se apoya prácticamente en todas las empresas que conforman el sector de la ciberseguridad en España. Me gustaría destacar como una parte muy importante de nuestra cultura corporativa el hecho de que es una entidad esté siempre abierta a la colaboración y cooperación, lo que se ha materializado, por citar algunos ejemplos, en una estrecha relación con el Ministerio del Interior, con la Organización de Estados Americanos o con entidades privadas como Microsoft.

3. ¿Existen herramientas y programas eficaces y efectivos para la colaboración público-privada en este país? Y desde el punto de vista de la propia Administración, ¿considera que el intercambio de información so ciber-amenazas es fluido a nivel interadministrativo?

Quizás hace unos años esta pregunta fuera más fácil de contestar, porque la dificultad existía y era muy complicado articular estructuras fiables de colaboración entre lo público y lo privado. Hoy tenemos la suerte de conocer numerosas actividades y líneas de trabajo cuyo principal enfoque o cuyo pilar más importante es la colaboración público privada. En INCIBE nos hemos subido al carro con apuestas efectivas de este tipo de colaboraciones, mediante convenios bilaterales con entidades nacionales e internacionales del ámbito de la Ciberseguridad, mediante acuerdos con asociaciones o patronales que representan la voz de la industria, y mediante la participación en diferentes foros que auspician estas colaboraciones. En nuestra opinión estas sencillas herramientas son efectivas porque devuelven a ambas partes un importante retorno de la inversión de esfuerzos. En materia del intercambio de información es vital la predisposición por el sector privado a colaborar activamente con la Administración. En nuestro caso disponemos de numerosas colaboraciones relativas al intercambio de información en Ciberseguridad, información que nutre nuestros sistemas de inteligencia en Ciberseguridad y que con la inestimable ayuda del sector privado se convierte en una fuente de datos fundamental para la resolución de incidentes, la detección temprana de amenazas, ataques, nuevos riesgos, la prevención y protección de ciudadanos, empresas, sectores estratégicos y críticos, la red académica, en definitiva los públicos a los que prestamos nuestros servicios públicos. Para nosotros el intercambio de información interadministrativo sobre ciberamenazas es una realidad que ya llevamos trabajando con éxito desde 2012 que firmamos un sólido y potente convenio con la Secretaría de Estado de Seguridad del Ministerio del Interior, y cuyos frutos son principalmente el CERT de Seguridad e Industria (CERTSI_), pilar fundamental de la Estrategia de Ciberseguridad Nacional, y la lucha más efectiva contra el ciberdelito y el ciberterrorismo. Así mismo y mediante la citada Estrategia, pero también a través de la Agenda Digital Española y el Plan de Confianza Digital del que participamos activamente se están articulando mecanismos aun más efectivos de colaboración público-público, y público-privado.

"...es vital la predisposición por el sector privado a colaborar activamente con la Administración"

4. Desde su punto de vista, ¿cree que las políticas y marcos nacionales existentes agilizan y a animan al tejido empresarial español a compartir los incidentes de seguridad que sufren? ¿Qué se podría hacer para catalizar esta tarea?

Nuestra enfoque y labor en esta materia tienen un acercamiento muy práctico. Somos capaces de detectar y tratar más de 8-9 millones de eventos de Ciberseguridad al día (IPs maliciosas, enlaces, dominios, malware, vulnerabilidades, fugas de información, etc.).

No en vano el año 2014 tratamos más de 1.800 millones de este tipo de eventos. Esta capacidad que seguimos construyendo y generando día a día redunda en un potente servicio de detección de nuevos incidentes que en muchas ocasiones con el desconocimiento de la víctima o del afectado conseguimos notificarle e indicarle los mejores mecanismos de mitigación o resolución del mismo. Evidentemente es más práctico aún que las propias empresas se sientan en un ambiente de confianza con la Administración y sepan que pueden confiar en nosotros, en nuestra experiencia y conocimiento, pero también en nuestro tratamiento de la confidencialidad y la privacidad, para no dañar su reputación y su modelo de negocio. En ese ambiente de confianza, y en un servicio de alta calidad entendemos que dicho tejido empresarial será aún más proclive a comunicar y compartir información sobre incidentes, ataques, amenazas, etc., porque buscan también un apoyo en la resolución. Por citar un ejemplo muy exitoso desde la puesta en marcha del CERT de Seguridad e Industria hemos firmado acuerdos con más de 40 empresas estratégicas y hemos resuelto más de 120 incidentes cibernéticos. A raíz de cada uno de ellos el lazo de relación se afianza y crece. Cuando nos acercamos a entornos empresariales más cerca de la PYME y sobre todo de la micro PYME entonces el esfuerzo se concentra más en una prestación de servicios más cercana y efectiva, en la concienciación, en la tutela en Ciberseguridad, que es el papel que muchas de estas empresas nos reclaman.

5. Desde INCIBE, ¿se plantea el desarrollo de un marco de control y seguridad básico para empresas al estilo del *"Cyber Essentials"* británico? En caso afirmativo, ¿qué tipo de medidas cree que deberían ser tomadas desde la Administración para facilitar su adopción?

Correcto. Es una nuestra principales fuentes de referencia e inspiración, que añadida a la referencia estadounidense por ejemplo de la Federal Trade Commission, se unen a otras fuentes o referencias que utilizamos para el diseño y desarrollo de nuestros servicios, y su continua evolución. Durante 2014 y parte de 2015 hemos hecho un importante esfuerzo en esta materia con un catálogo nuevo de servicios de Ciberseguridad para empresas, que no sólo incluyen la resolución de incidentes, sino una nueva línea de contenidos y materiales que ahondan en la interactividad tales como un kit de concienciación en Ciberseguridad autodesplegable por la propia empresa, un servicio de autodiagnóstico ligero, herramientas de Ciberseguridad, o servicios que inicialmente puestos en marcha con el foco en los ciudadanos como el Servicio Antibotnet, se están prestando ya para el entorno empresarial. Durante lo que queda de año 2015 y 2016 estamos trabajando en la mejora de estos servicios incorporando aún más interactividad, por ejemplo a través de la gamificación, la incorporación de videotutoriales y la segmentación de contenidos en itinerarios específicamente configurados para diferentes sectores. Adicionalmente estamos ya trabajando en el primer MOOC de Ciberseguridad para empresas.

6. Más allá de las empresas cotizadas, en lo que respecta al estado general de ciberseguridad del resto de empresas españolas ¿considera que son conocedoras de su nivel de exposición y de los ciber-riesgos inherentes a su actividad? ¿Qué recomendaciones generales aportaría?

Según nuestra visión en INCIBE y por el crecimiento de resolución de incidentes en los dos últimos años, 18.000 en 2014 y ya vamos por más de 62.000 en 2015, también debido a que detectamos más situaciones de riesgo, ataques y amenazas, consideramos que el entorno empresarial va siendo consciente, aunque lentamente, de la exposición y de los riesgos en la Red. De hecho este año incidentes como el ransomware, malware diseñado para una vez infectada una infraestructura o sistemas cifra la información y luego el ciberdelincuente pide un rescate para recuperar la información, están haciendo que la empresa sea consciente de manera reactiva al enfrentarse a estas situaciones, pero tenemos que seguir trabajando la parte preventiva más que la reactiva, y eso pasa por trabajar mucho en la sensibilización, en la concienciación, en ofrecer servicios efectivos, y sobre todo que nos conozcan más. Por eso estamos trabajando en hacer más potentes los diferentes canales web (*www.incibe.es*, *www.osi.es*), redes sociales, etc., y tener más presencia en medios de comunicación generalistas ya que en el sector tecnológico el posicionamiento de INCIBE es ya muy considerable. Estamos trabajando en una ambiciosa campaña de difusión con lenguaje y mensajes sencillos, prácticos, bien enfocados, y que sirvan para sensibilizar y concienciar pero también para dar a conocer dichos servicios y que en definitiva hagan un uso más fuerte de nuestras capacidades. Una empresa debe según nuestra experiencia integrar en su modelo de negocio la Ciberseguridad, porque previniendo los ataques es más fácil recuperarse frente a los incidentes, porque con unos niveles de preparación o ciberresiliencia básicos es factible resistir a los intentos por parte de ciberdelincuentes de perjudicar nuestra actividad o conseguir un perjuicio económico. Una infraestructura protegida con herramientas de Ciberseguridad, bien actualizada en cuanto a las necesidades de plataformas, sistemas operativos, software, etc., unos empleados sensibles y conscientes de ciertos riesgos, y una organización informada, es una empresa más cibersegura y ciberresiliente. En nuestros servicios de Protege Tu Empresa *(https://www.incibe.es/ciberseguridad/empresas/)*, tenemos muchos recursos enfocados en esta filosofía.

" tenemos que seguir trabajando la parte preventiva más que la reactiva "

7. Desde el punto de vista del Instituto, ¿se plantea fomentar la adopción por parte de la empresa española de estrategias de transferencia del ciber-riesgo a través de productos aseguradores (ciber-seguros)?

Es una posibilidad a tener en cuenta, sobre todo para empresas cuya reputación digital o imagen online son un factor muy importante de su modelo de negocio. La transferencia del ciber-riesgo es un paso en la madurez que se adopta cuando previamente has realizado un análisis de riesgos, y en base a un análisis

de impacto de los mismos, y el presupuesto que has de invertir en contramedidas te lleva a decidir que la mejor estrategia es transferir dicho riesgo a un tercero en formato de un ciber seguro. Lo que creemos en este aspecto es que dicho análisis tiene que ser muy específico, y que debemos suscribir un seguro que sea capaz de ayudar a mitigar el impacto producido por un incidente que se ha materializado y que ha producido un importante perjuicio en nuestra actividad. No es lo mismo que la imagen de una empresa se vea afectada por la actividad de hacktivistas por ejemplo y que con ello la confianza de sus clientes baje y por lo tanto también dicha empresa pierda esa clientela, que por un incidente la actividad se pare y estemos hablando de una línea de producción. Para nosotros medir es fundamental y por ello por ejemplo hemos puesto en marcha un modelo de medición de indicadores de ciberresiliencia que entre otras cosas ayuda a saber cómo estamos de maduros y resistentes frente a un ciberataque.

8. ¿Qué cautelas mínimas recomendaría a cualquier empresa española de cara a afrontar los riesgos derivados de la exposición al medio digital?

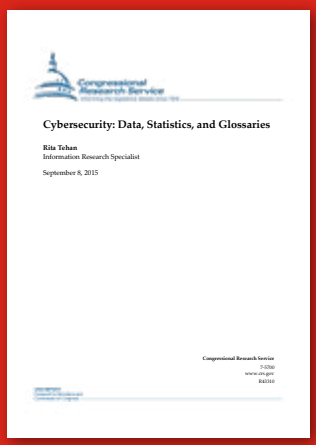
Como citaba anteriormente todos nuestros activos deben ser analizados desde el punto de vista de su valor para la organización: información, infraestructura, nuestras personas o empleados, …y todos ellos deben tener alguna contramedida o medida de Ciberseguridad, infraestructura correctamente mantenida y actualizada, monitorizada, protegida con ciertas herramientas de seguridad, la información salvaguardada, copias de seguridad, control anti fugas, y las personas deben saber que son parte de este todo, deben tener un backup de su rol en la empresa, rotar funciones, segmentar funciones, deben tener una formación en Ciberseguridad adaptada al puesto…Una empresa que se toma en serio su modelo de negocio debe tomarse en serio la Ciberseguridad y contar también con servicios profesionales en la materia. Y por último esta empresa debe estar informada igual que lo está por temas legales o por su propio negocio. Cuanta mayor sea la dependencia tecnólogica mayor debe ser esta realidad en Ciberseguridad, estar preparados, estar prevenidos, y ser resilientes a los ciberataques.

5 Informes y análisis sobre ciberseguridad publicados en septiembre de 2015

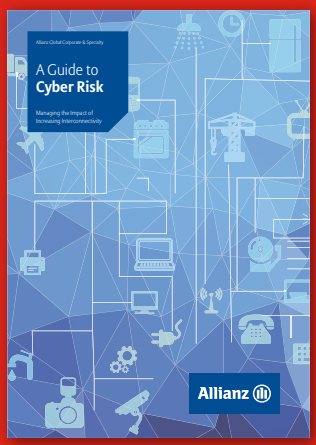
ENISA Cyber Europe 2014 (ENISA)

Anual Incidents Report 2014 (ENISA)

Cybersecurity: Data, Statistics, and Glossaries (U.S Congress Library)



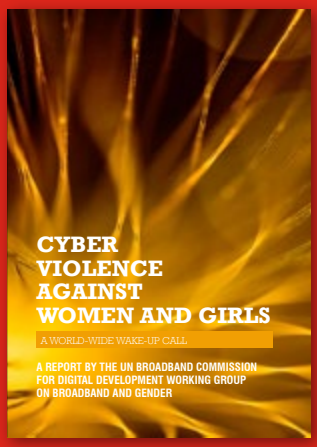
A Guide to cyber risk (ZURICH)



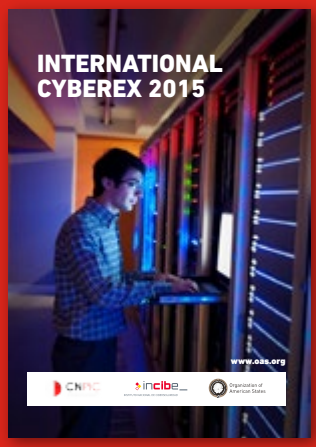
Beyond the build: Delivering outcomes through cyberespace (U.S CyberCommand)

Medidas de seguridad contra ramsonware (CCN-CERT)

Cyberviolence against women and girls (United Nations)



International Cyberex 2015 (INCIBE)



6 HERRAMIENTAS DEL ANALISTA: Diffy

Como ya hizo Facebook en 2007, cuando liberó *Thrift Technology*, una herramienta usada a nivel interno por la red social para analizar el código fuente en busca de vulnerabilidades, Twitter a presentado este mes *Diffy*. A diferencia de la aproximación de Facebook, Diffy es una herramienta totalmente abierta y gratuita.

Diffy es una herramienta de código abierto que encuentra automáticamente errores de programación en Apache Thrift y servicios basados en HTTP. Requiere de una configuración mínima y es capaz de encontrar bugs en el código sin necesidad de diseñar complejos conjuntos de pruebas por parte de los programadores.

En arquitecturas orientadas a servicio como la de *Twitter*, es habitual tener un gran número de servicios TIC que evolucionan a un ritmo muy rápido. A medida que se añaden nuevas características con cada versión, el código existente es inevitablemente modificado a diario siendo factible cometer errores de programación que puedan suponer un problema de seguridad.

Desarrollar pruebas unitarias ofrece cierta confianza, pero escribir un buen conjunto de pruebas puede llevar más tiempo que escribir el código en sí. Adicionalmente, las pruebas unitarias ofrecen cobertura para ámbitos restringidos a pequeños segmentos de código, pero no abordan el comportamiento agregado de un sistema compuesto centenares o miles de líneas de código.

Así pues, Diffy encuentra errores potenciales en un servicio ejecutando instancias paralelas de la nueva versión de un código fuente y la antigua. Se comporta como un proxy propagando los inputs que recibe a cada una de las instancias en ejecución para analizar su comportamiento. A continuación, compara las respuestas de ambas versiones del código e informa de cualquier problema surgido a partir de estas comparaciones.

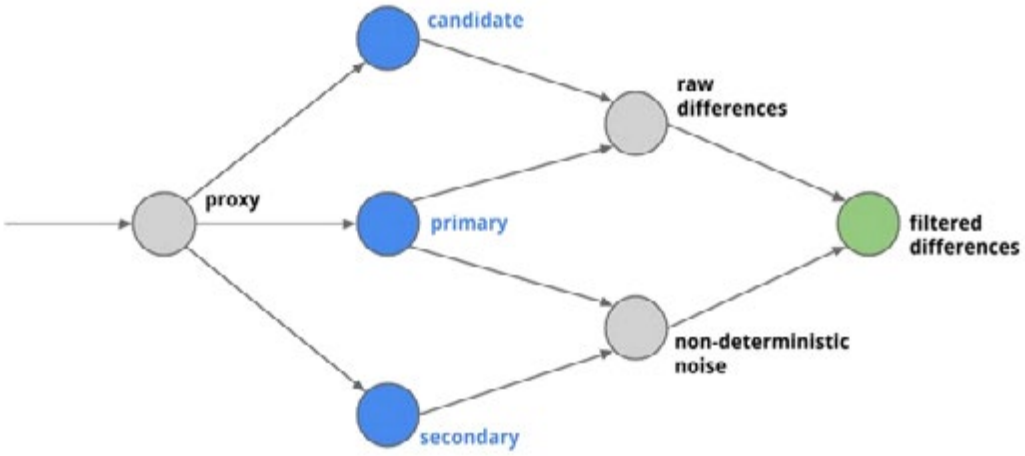


Ilustración Diagrama de funcionamiento de Diffy

La premisa para Diffy es que si dos programas o servicios devuelven respuestas “similares” para un conjunto suficientemente amplio y diverso de solicitudes, las dos implementaciones pueden ser tratadas como equivalentes y la nueva versión sería aceptada como buena.

En definitiva, Diffy permite a los desarrolladores que el seguimiento de errores potenciales entre actualizaciones de código sea mucho más sencillo de una forma abierta y gratuita.

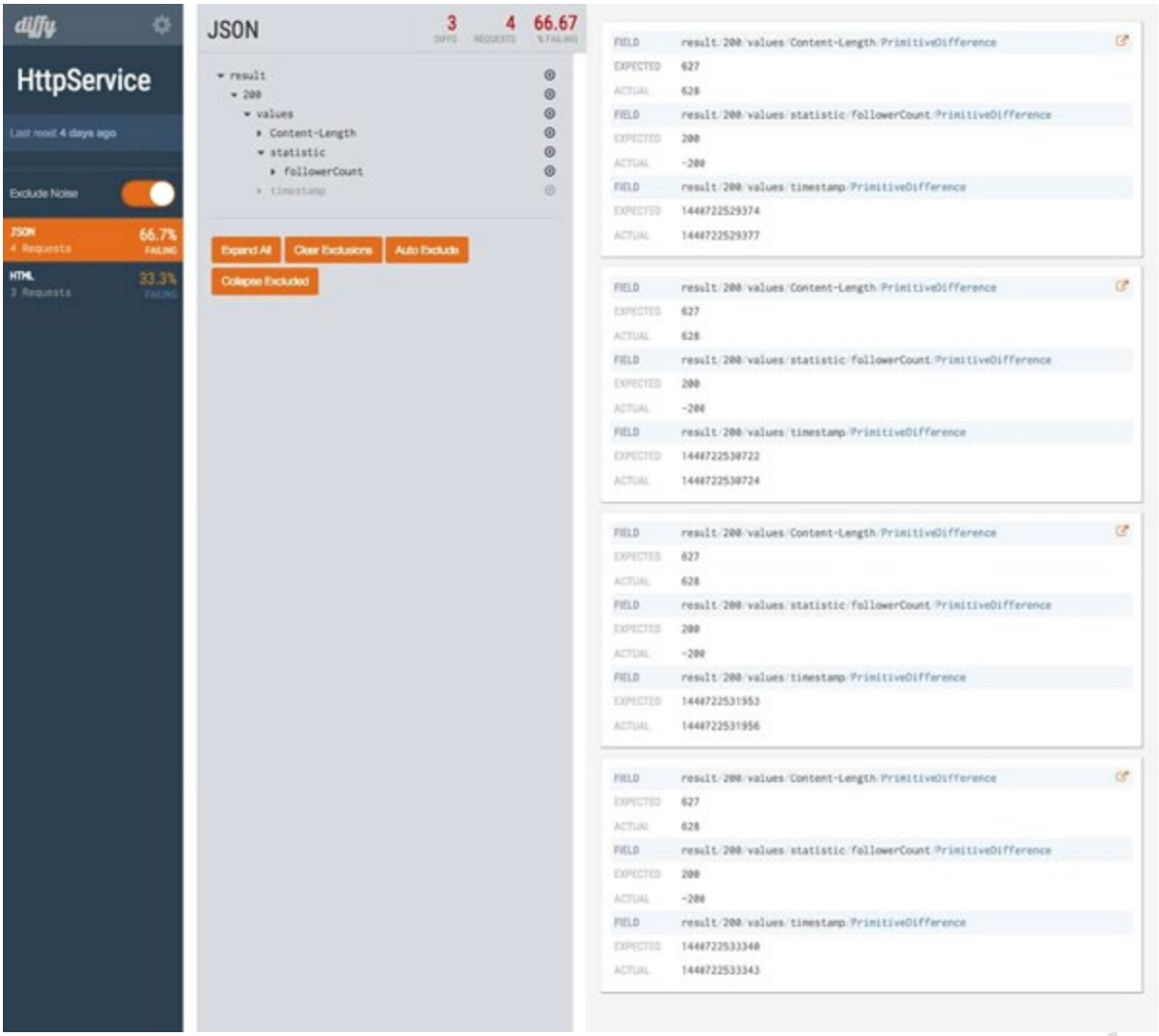


Ilustración 2 Screenshot de la intefaz de Diffy

7 Análisis de los Ciberataques del mes de septiembre de 2015

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

La llegada del otoño no ha supuesto una reducción de la actividad maliciosa en el ciberespacio, como sucedía en años anteriores. Durante el mes de septiembre ha existido un claro actor protagónico: la aplicaciones móviles maliciosas provenientes de markets de "confianza". También hemos presenciado una gran operación de ciber-espionaje a través de implants hardware en elementos de electrónica de red.

CIBERCRIMEN

A mediados de mes, el fabricante de seguridad Palo Alto identificaba una treintena de apps móviles maliciosas en Apple Store, muchas de ellas muy populares en China con un gran número de descargas.

Una versión troyanizada de XCode, el framework con el que se desarrollan las aplicaciones para entorno iOS, distribuido a través de diversos foros, ha sido usada para compilar y enviar a la App Store diferentes aplicaciones durante varios meses. El vector de ataque, denominado XCodeGhost, permite a un atacante remoto recibir información del dispositivo infectado (IMEI, credenciales, IP, etc.).

Si bien Apple ha retirado las aplicaciones afectadas, algunas de ellas, como WeChat, con más de 600 millones de descargas, esta infección de malware ha supuesto uno de los mayores problemas de seguridad en el ecosistema de Apple Store.

A finales de mes, *Patreon*, la plataforma de micromecenazgo que está consiguiendo *bastante repercusión* por su concepto, al acercar a los fans a sus artistas, permitiéndoles interactuar con ellos y ayudarles mediante micropagos, fue victima de un ataque que ha supuesto la exposición de 15 GB de contraseñas, mensajes privados, registros de donaciones y hasta código fuente.

A pesar de que Patreon implementa un algoritmo llamado de cifrado denominado "bcrypt", a priori seguro, **los atacantes podrían haber utilizado vulnerabilidades en el código fuente** para conseguir decodificar las contraseñas de los usuarios, prácticamente lo mismo que hicieron hace unos meses otros atacantes en Ashley Madison.

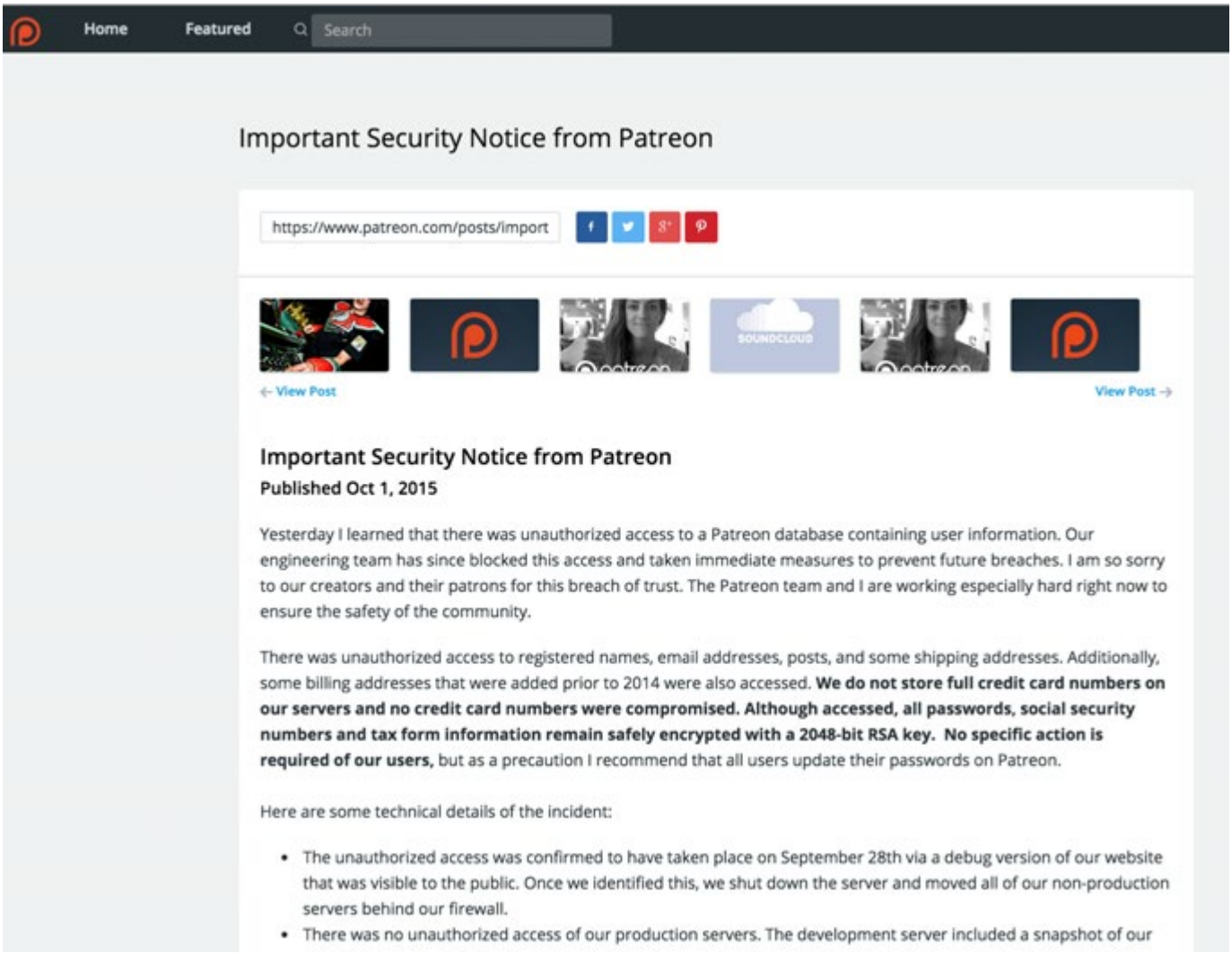


Ilustración 1 Mensaje explicativo de Patreon tras el ataque

La página web de la Agencia Nacional de Delincuencia del Reino Unido, nationalcrimeagency.gov.uk, se vio afectada brevemente por una *denegación de servicio distribuido (DDoS) el pasado 1 de septiembre*. Pocos días después, la propia agencia anunció el arresto de seis adolescentes por el uso de un servicio DDoS comercial. Lizzard Squad, el grupo detrás del servicio usado en el ataque, reclama la responsabilidad en Twitter, y ha aprovechado la ocasión para convertirlo en un anuncio de la próxima versión del servicio.

Continuando con los DDoS, algunas grandes corporaciones e instituciones del Reino Unido, como Lloyds Bank y BAE, han informado de un "aumento marcado" en ese tipo de ataques por parte del grupo de extorsionadores de bitcoins DD4BC, que ha estado en funcionamiento desde el año pasado. Esta proliferación ataques parecen ser identificadas por otras entidades . *Un estudio publicado por Akamai* identifica 114 ataques atribuidos a DD4BC contra clientes de la compañía desde abril de 2015, con 41 casos solamente en junio de este año. En comparación, sólo se han registrado 5 ataques entre enero y febrero de este año.

Tras el ataque que sufrió el verano pasado en el servicio de emails no clasificados del Pentágono, en esta ocasión un *grupo de atacantes se han infiltrado en los sistemas del departamento de alimentos del citado organismo*, comprometiendo un número no determinado de datos bancarios de empleados.

Todos los empleados han sido notificados a fin de que monitoricen sus cuentas bancarias en los días subsiguientes al ataque con el objetivo de identificar movimientos sospechosos, ya se han detectado muchos movimientos de cuentas ilegítimos según ha reportado la Force Protection Agency del Pentágono a algunos medios de comunicación norteamericanos.

CIBERESPIONAJE

Trend Micro y ClearSky han publicado un análisis conjunto en el que se documentan las acciones de un grupo tras un APT que consideran relacionado con el gobierno iraní.

Desde partir de abril de 2014 y hasta junio, Trend Micro y ClearSky analizaron la información recogida por otras empresas de seguridad como iSIGHT y FireEye junto con sus propios datos y llegaron a la conclusión de que un grupo apodado como Rocket Kitten tiene vínculos con el gobierno iraní.

Su investigación identifica un APT dirigido contra objetivos estratégicos de varios gobiernos extranjeros, instituciones académicas, y sobre todo, objetivos ubicados en Israel.

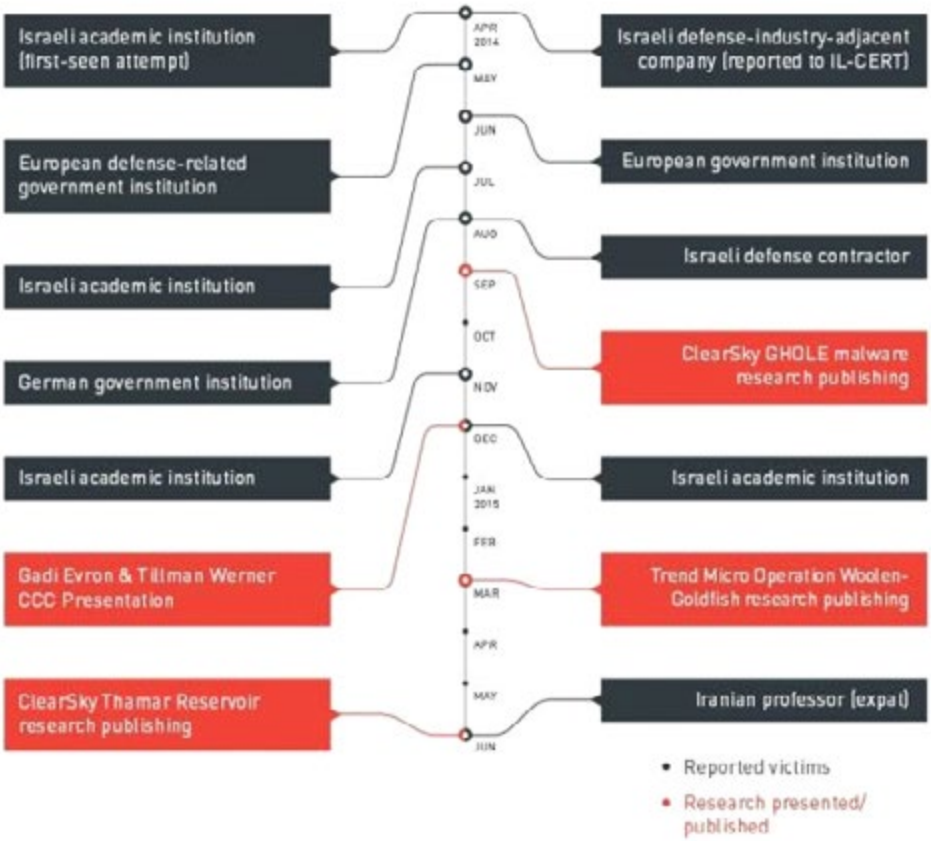


Ilustración 2 Timeline del APT Rocket Kitten

A mediados de mes, *FireEye desveló los detalles de una campaña que implica la modificación fraudulenta del firmware de routers CISCO* que puede ser utilizado para mantener la persistencia dentro de la red de la víctima a través de ese implant hardware. La campaña, denominada **Synful Knock** a ha afectado a por lo menos 79 dispositivos en 19 países.

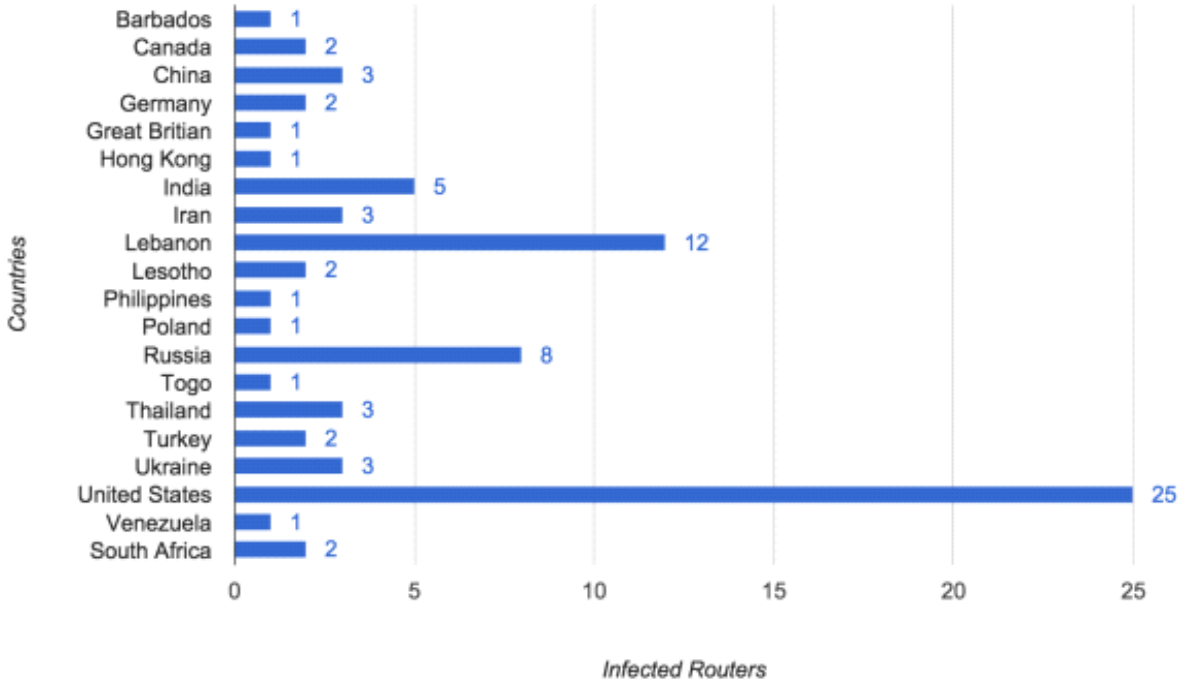
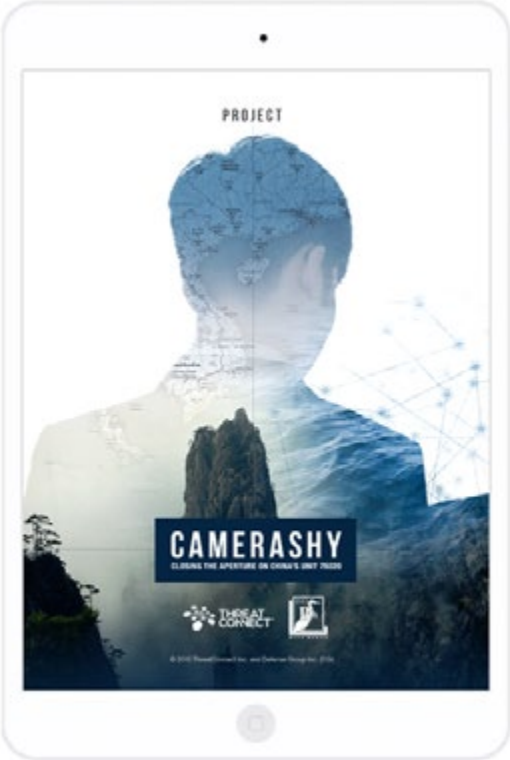


Ilustración 3 Routers Cisco infectados por el implant malicioso

Ge Xing, también conocido como "GreenSky27," es el Nick de un presunto miembro de la unidad 78020 del Ejército Popular de Liberación (EPL), un grupo de hackers patrocinados por el estado chino. La persona fue identificada a través de una investigación conjunta realizada por dos compañías de seguridad. Ge Xing y otros miembros reúnen inteligencia de fuentes militares y políticas para soportar los intereses de China en el Mar Meridional de China.



La investigación, desarrollada por ThreatConnect en colaboración con Defense Group Inc., ha denominado la operación *CameraShy* mediante un APT dirigido denominado 'Naikon'

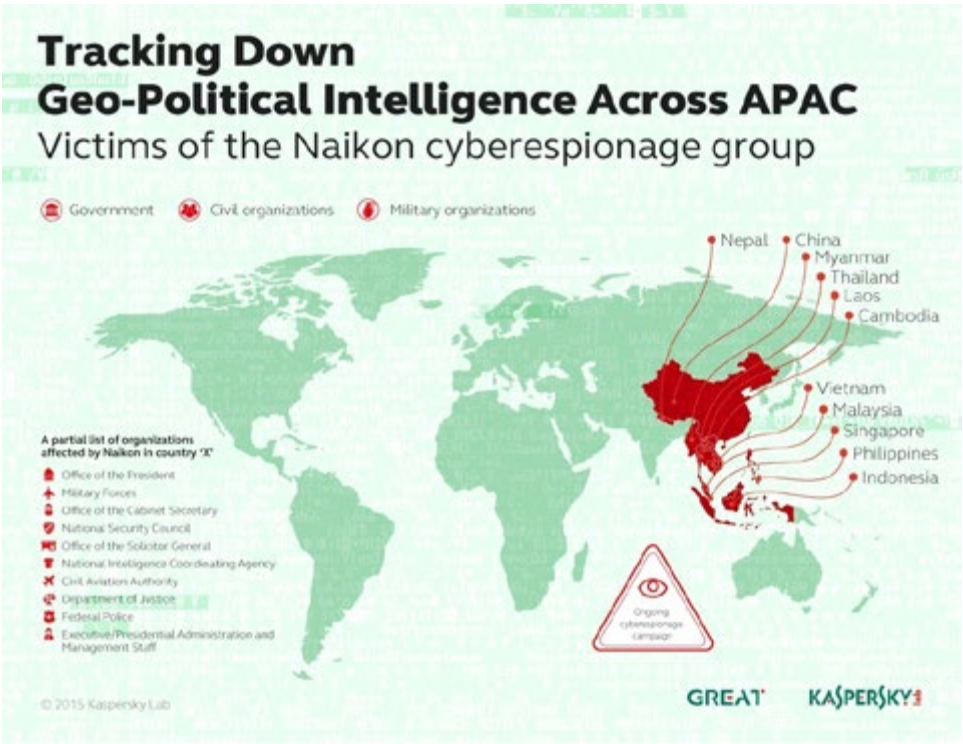


Ilustración 4 Mapa de víctimas de Naikon

El 11 de septiembre, una investigación realizada por el GCHQ británico *informó del descubrimiento del robo de información clasificada* por parte de extremistas vinculados al Daesh. Dicha información estaba en poder de algunos de los ministros más veteranos del gobierno de Cameron, incluyendo a Theresa May, Ministra de Interior.

Se piensa que al menos uno de los cabecillas del robo de datos fue eliminado por un ataque aéreo con drones en una operación llevada a cabo por el gobierno británico tras el incidente.

A través del ciberataque, y la información sustraída de las oficinas privadas de los ministros, los atacantes podrían haber descubierto la agenda de eventos públicos y privados así como los planes logísticos de la familia real y de importantes miembros de gobierno.

A comienzos de mes, *un medio de comunicación norteamericano* ha tenido acceso a diversos registros federales a través de la Freedom of Information Act mostrando que un periodo de 48 meses que, comenzando en 2010 y finalizando en octubre de 2014, se registraron más de 1.300 ciberataques sobre infraestructuras críticas energéticas estadounidenses, siendo 159 de ellos exitosos.

Los informes de incidentes presentados por funcionarios federales y subcontratas desde finales de 2010 al Centro Conjunto de Coordinación de Ciberseguridad del Departamento de Energía norteamericano muestran una tendencia casi constante de intentos de acceso a los los sistemas de información críticos que contienen datos sensibles sobre la red eléctrica de la nación, arsenales de armas nucleares y la laboratorios de investigación energética.

Estos ataques coinciden con los ciberataques, de autoría desconocida, que a lo largo del mes se han dirigido contra infraestructura de comunicaciones críticasde EEUU, llegando a cortar el backbone de fibra óptica de Internet en California.

HACKTIVISMO

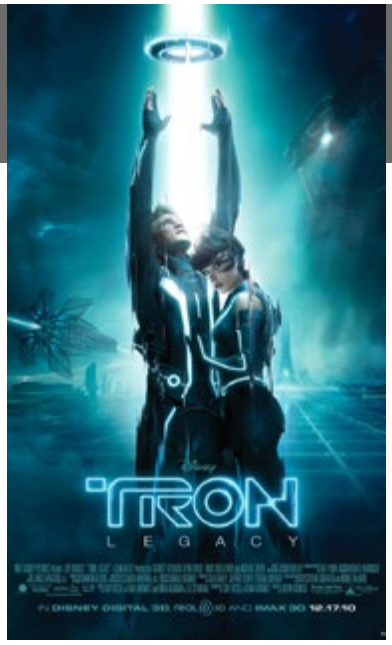
En el plano del ciber activismo, la web oficial del Kremlin (http://kremlin.ru) fue víctima de un ataque de DDoS masivo. El ataque se llevó a cabo simultáneamente con otro ataque que se dirigió contra sitio web de la Comisión Electoral Rusa, llevándose a acabo ambos ataques el Día Nacional de Elecciones.

Ilustración El portavoz del gobierno ruso, Dmitry Peskov, en la rueda de prensa en la que anunciaba el incidente

El pasado día 2 de septiembre, un grupo de atacantes que dicen ser parte del Estado Islámico, realizaron un defacement web del sitio de la Junta de Educación del condado de Wayne, en el estado de Virginia. Mediante este ataque, los visitantes de la web eran redirigidos a una web que promuevía el terrorismo islámico.

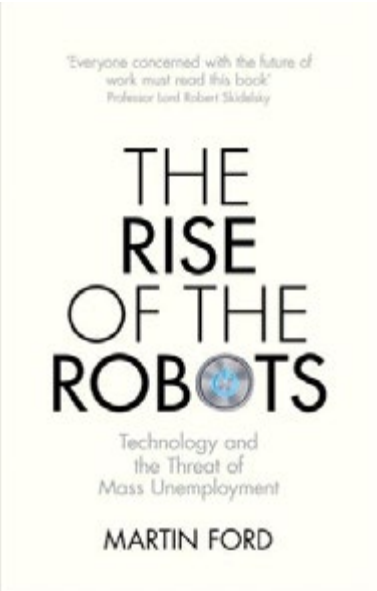
8 Recomendaciones

8.1 Libros y películas



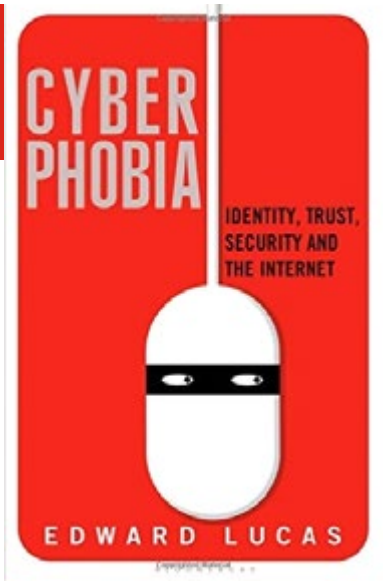
Película:
TRON LEGACY

Sinopsis: Cuando un experto programador investiga la desaparición de su padre, se encuentra de repente inmerso en un peligroso y salvaje mundo surrealista, un mundo paralelo donde su padre ha vivido durante 25 años. Con la ayuda de una joven, padre e hijo emprenden un viaje a vida o muerte, a través de un sofisticado universo cibernético. Secuela del clásico de culto de 1982.



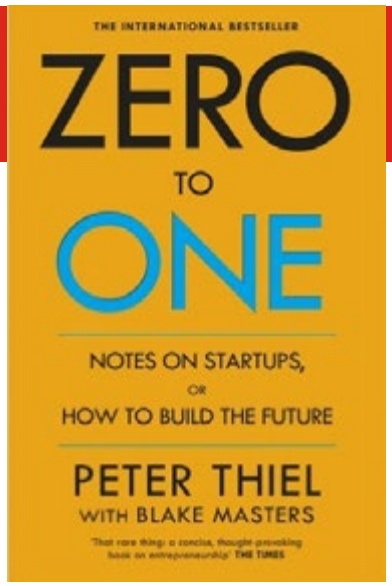
Libro:
THE RISE OF THE ROBOTS

Autor: Martin Ford
Num. Paginas: 352
Editorial: Oneworld Publications
Año: 2015
Precio: 15.00 Euros
Sinopsis: El autor alerta sobre la evolución de los robots y como estos pueden afectar al futuro de la humanidad.



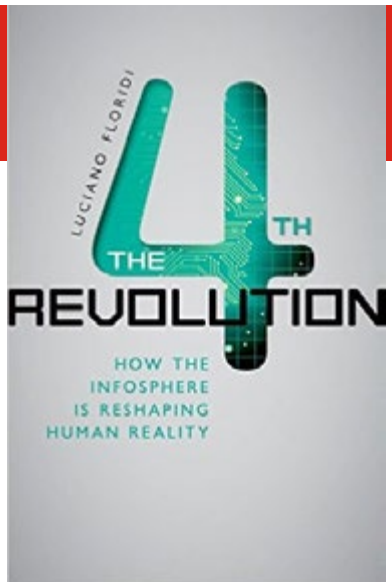
Libro:
CYBERPHOBIA: IDENTITY, TRUST, SECURITY AND THE INTERNET

Autor: Edward Lucas
Num. Paginas: 336
Editorial: Bloomsbury
Año: 2015
Precio: 20.00 Euros
Sinopsis: El autor analiza las principales amenazas de internet y propone un conjunto de estrategias para defendernos de ellas.



Libro:
ZERO TO ONE

Autor: Peter Thiel
Num. Paginas: 224
Editorial: Virgin Books
Año: 2015
Precio: 20.00 Euros
Sinopsis: Peter Thiel, fundador de PayPal y Palantir, nos explicas las claves para crear una start-up tecnológica de éxito.



Libro:
THE FOURTH REVOLUTION

Autor: Luciano Floridi
Num. Paginas: 272
Editorial: OPU OXFORD
Año: 2014
Precio: 13.00 Euros
Sinopsis: El autor nos explica como las nuevas tecnologías condicionan las relaciones humanas.

8.2 Webs recomendadas

https://cybersecuritymonth.eu/
Como motivo del mes de la ciberseguridad, ENISA nos conciencia en el uso responsable del ciberespacio.

http://cybersecforum.eu/en/
OTAN y el Ministerio de Asusntos Exteriores polaco organizaran CYBERSEC.

https://www.b-ccentre.be/
BCCENTRE es un centro de excelencia en la lucha contra el cibercrimen financiado por la Unión Europea.

https://www.sans.org/security-resources/blogs
Sito web de los Blogs soportados por el SANS

http://blog.isc2.org/
Blog del International Information System Security Certification Consortium (ISC)²

http://www.isaca.org/Blogs/Pages/default.aspx
Sitio web de los blogs de la ISACA.

8.3 Cuentas de Twitter

@securetech_arg

@CERTSI_

@CERT_Polska_en

@CyberSecMonth

@CYBERSECEU

@Foro_Seguridad

9 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
1-3 octubre	Albacete	NNC5ED	Navaja Negra	http://navajanegra.com/
1 Octubre	Washington	Washington Post	The Washington Post Cybersecurity Summit	http://www.washingtonpost.com/blogs/post-live/wp/2015/07/09/live-oct-1-2015-cybersecurity-summit/
5-7 octubre	Berlin	CRITIS	The 10th International Conference on Critical Information Infrastructures Security	www.critis2015.org
8 Octubre	Madrid	Isaca	La Ciberseguridad: Una Responsabilidad de Todos	http://isacamadrid.fikket.com/event/cibertodos-2015-la-ciberseguridad-una-responsabilidad-de-tod-s
14 Octubre	Madrid	ISMS Forum	IV Foro de la Ciberseguridad del Cyber Security Center	https://www.ismsforum.es/evento/programa.php?idevento=633
15 Octubre	Madrid	Red Seguridad	Jornada de Continuidad de Negocio	http://www.redseguridad.com/revistas/red/eventos/continuam2015/continuam2015_programa.pdf
19-21 October	Dublin	WorldCIS-2015	World Congress on Internet Security	http://www.worldcis.org/
20-21 Octubre	Leon	INCIBE	9 ENISE	https://www.incibe.es/enise/programa/
21-23 octube	Leon	Meridian	Conferencia Meridian 2015	http://meridian2015.es/
22 Octubre	Madrid	RSA	RSA Advanced Cyber Defense Summit	http://spain.emc.com/campaign/global/forum2015/event.htm
21-23 Octubre	Buenos Aires	Ekoparty	Ekoparty	https://www.ekoparty.org/
22-23 octubre	Santiago de Chile	8.8	8.8	http://8dot8.org/

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