JUNIO 2015 / Nº 4

CIBER elcano

REAL INSTITUTO elcano ROYAL INSTITUTE

Desarrollado por:

THIBER

INFORME MENSUAL DE CIBERSEGURIDAD

REAL INSTITUTO
elcano
ROYAL INSTITUTE

Índice

1 COMENTARIO CIBERELCANO:

Los cibercomandos y la segregacion de funciones

AUTOR: Dr. José Ramón Coz Fernández. Analista Internacional THIBER.
Security Manager y Auditor en PMIC-OTAN

La segregación de funciones es un asunto prioritario para muchos profesionales de todo el globo, desde los responsables de su cumplimiento hasta los ejecutivos y decisores de más alto nivel. En el campo de la ciberdefensa este concepto es fundamental, puesto que debe existir una clara distinción entre el responsable de elaborar las normas en materia de ciberseguridad y el responsable de velar por su cumplimiento.

No obstante, en su aplicación práctica es un asunto mucho más complejo. El concepto de segregación de funciones tiene sus orígenes en el principio de que ningún actor puede realizar todo el proceso sin ningún tipo de control intermedio. A modo de ejemplo, ninguna persona debería tener pleno acceso a los sistemas de tal forma que pudiera ejecutar transacciones globales en todo el proceso de la organización sin controles o autorizaciones intermedias.

Si quien establece la norma se encarga de su vigilancia, los riesgos que se asumen son enormes. En este sentido, ¿se imagina el lector que en un régimen democrático el poder legislativo y el judicial estuviera compuesto por los mismos integrantes? Sin embargo, pese a que estos conceptos están muy extendidos, no en todas las organizaciones se ponen en práctica con la debida diligencia.

En el caso de los Cibercomandos, a nivel internacional, en casi todos los países tienen una serie de funciones muy similares. Tras analizar un conjunto relevante de países, casi todos ellos tienen como responsabilidad llevar a cabo operaciones relacionadas con la defensa. En el caso de operaciones conjuntas, actúan como soporte TIC de otros mandos que operan en las otras dimensiones (tierra, mar, aire o espacio), y en el caso de las ciberoperaciones, las lideran a la vez que reciben un soporte reciproco del resto de la organización global de defensa.

Los Cibercomandos suelen estar segregados de las organizaciones responsables de monitorizar la seguridad de la información. Esto es vital para garantizar que el ciclo de vida de los procesos relacionados con la seguridad tenga una garantía mínima de control. Pero es que, además, en los Cibercomandos, como usuarios de sistemas, herramientas y procesos, para que se asegure un riesgo aceptable en el desempeño de sus misiones, estas herramientas, sistemas y procesos deben de ser monitorizados por organizaciones que otorguen unas garantías mínimas de control.

Lo que siempre se cumple en los países más avanzados en Ciberdefensa, y como requisito obligatorio ligado al importante concepto de segregación de funciones, es que las organizaciones responsables de diseñar y elaborar las normas y las políticas relacionadas con la seguridad de la información están segregadas de los mandos operativos y de las organizaciones que monitorizan y velan por el cumplimiento. Esto es vital para el buen funcionamiento y control en las organizaciones. Y es que el riesgo mayor se produce cuando la propia organización responsable de monitorizar la seguridad es la responsable de elaborar las políticas y los procedimientos relacionados.

Los estándares internacionales abogan por el cumplimiento de esta segregación de funciones y establecen unas buenas prácticas para su cumplimiento. En el caso de la Asociación de Auditoría y Control de Sistemas de Información (ISACA) se proponen roles muy específicos y detallados que deben ser segregados para garantizar un riesgo aceptable en el funcionamiento de los sistemas, las comunicaciones y las TIC.

Sin embargo, como el mundo ideal no existe, en algunos casos los Cibercomandos están integrados dentro de las propias organizaciones de monitorización de la seguridad de la información. Por supuesto, este hecho sucede también en muchas medianas y pequeñas empresas y organizaciones, donde los usuarios finales de los sistemas y los operadores de procesos críticos del negocio comparten en algunos casos labores de monitorización de la seguridad de la información.

"Los Cibercomandos suelen estar segregados de las organizaciones responsables de monitorizar la seguridad de la información"

Al final, los presupuestos y el personal son limitados y, por tanto, es imposible segregar todas las funciones que serían necesarias. En el caso de los Cibercomandos se da, además, el hecho de que muchas veces se comparten algunos perfiles similares en ambas organizaciones. Para este caso, en el que los mandos operativos, como puedan ser los Cibercomandos, tengan responsabilidades compartidas con la monitorización de la seguridad de la información, existe el concepto de Control Compensatorio, que permite poner medidas correctoras para que el ciclo sobre funciones críticas se cierre.

La forma de establecer este control compensatorio se lleva a cabo de multitud de formas, y una de ellas son los procesos de auditoria a los que se ven sometidos tanto los propios Cibercomandos como las organizaciones responsables de monitorizar la seguridad de la información. Estos procesos cobran cada vez una mayor relevancia en entornos muy críticos.

Las auditorias permiten descubrir en muchos casos esa falta de segregación de funciones y el establecimiento de controles compensatorios que permitan alcanzar un riesgo deseable. En multitud de países, a través de entidades independientes, se llevan a cabo estas auditorías, que incluyen grandes programas del entorno de la ciberseguridad.

Esta es una más de las razones por las que los grandes programas de ciberdefensa que se están llevando a cabo en los países más avanzados están sometidos a auditorias muy estrictas de cumplimiento, donde la segregación de funciones es uno de los aspectos más críticos a ser considerados.
Al final, los presupuestos y el personal son limitados y, por tanto, es imposible segregar todas las funciones que serían necesarias. En el caso de los Cibercomandos se da,

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
Los usos fraudulentos del Bitcoin

AUTORES: Félix Brezo. Analista de THIBER.
Yaiza Rubio. Analista de THIBER.

La proliferación de las distintas *criptodivisas* ha sido un fenómeno al alza desde la aparición de Bitcoin en el año 2009 fruto de la aceptación que están teniendo como medio de pago en distintas plataformas. A los tipos de cambio actuales, el valor hipotético de las unidades monetarias distribuidas de las más de seiscientas *criptodivsas* diferentes existentes *supera con creces los 3800 millones de dólares*, de los cuales al menos 3400 millones (el 88%) son atribuidos al valor de los catorce millones de bitcoins en circulación.

La novedad que presenta Bitcoin frente a otras alternativas es que se trata una divisa virtual que implementa un protocolo público de transacciones basado en una arquitectura peer-to-peer en la que no existen organismos centrales que regulen el valor o la cantidad total de monedas existentes, sino que su mantenimiento recae en la *capacidad computacional de su red de usuarios* para mantener el histórico de transacciones.

La gran cantidad de mercados existentes en la red y la posibilidad de cambiar estas por divisas convencionales a través de distintos portales, hacen de este método de pago una herramienta susceptible de ser utilizada para la comisión de delitos en la red. Además, sus características dificultan la atribución de las transacciones y la identificación de los responsables frente a la monitorización de las divisas convencionales.

En este sentido, Bitcoin está siendo utilizado como medio de pago para el rescate de los documentos secuestrados por *ransomware.* Aunque en el caso de algunas filtraciones de bases de datos corporativas *se han solicitado rescates de gran importe*, es habitual que se apueste por *rescates de tamaño medio o bajo*, pero siempre en órdenes de magnitud que el usuario infectado esté dispuesto a abonar.

De la misma forma, las *criptodivisas se están utilizando para monetizar otros servicios* que se pueden ofrecer fruto del despliegue de una *botnet* entre los que se incluyen el ofrecimiento de servicios DDoS, el envío de *spam*, la utilización de los equipos comprometidos para la navegación anónima a través de ellos, la venta de credenciales o incluso la minería encubierta de bitcoins en dichos equipos. Asimismo, en algunas plataformas se utiliza el Bitcoin para remunerar servicios de *hacking* bajo demanda, así como para la compraventa de *exploits*.

El uso de estas monedas propicia un escenario en el que la sustracción de monederos virtuales acapara un interés creciente para los grupos dedicados al cibercrimen ya que en ellos se almacenan cantidades económicas de más fácil sustracción que el dinero electrónico convencional.

En función del tipo de cartera escogido por el usuario para gestionar sus *criptodivisas*, *existen diferentes aproximaciones de cara a vulnerarlas.* Para las carteras en local, cuyas claves son almacenadas bajo control del usuario, un atacante con acceso al equipo podría efectuar transacciones hacia direcciones controladas por él si dichos ficheros no se encontraran protegidos.

En el caso de las carteras mentales, el ataque consistiría en la creación de diccionarios para generar de forma automática posibles direcciones y sus respectivas claves privadas. De esta manera, si un atacante identificara que uno de estos monederos contiene monedas, podría sustraerlas ya que contaría con la clave privada que firma las transacciones.

Las plataformas de terceros ofrecen servicios que facilitan el intercambio de divisas y la operación con bitcoins aun estando en equipos distintos al propio. El problema que conlleva es que con su utilización se delega en estas plataformas la administración de las claves y, por tanto, el control final de las monedas. De este modo, el usuario debe tener ciertas garantías de que se trata de un tercero confiable o de que mantiene unas medidas de seguridad proporcionales al valor de los activos que protegen.

Además, desde el punto de vista del usuario, el hecho de que estas plataformas no tengan implementadas sistemas de autenticación en dos pasos tanto para el acceso como para la emisión de transacciones, conlleva que la información procedente de una botnet convencional destinada al robo de credenciales podría ser más que suficiente para sustraer el dinero de las cuentas. Por todo ello, y a pesar de que solamente se utilicen actualmente en el 1% de las transacciones, se recomienda la utilización de las carteras multifirma porque para la emisión de transacciones se implica a todas aquellas direcciones que las hayan generado.

Pese a que apenas son *6500 establecimientos* los que aceptan Bitcoin como moneda de pago en todo el mundo, el volumen de transacciones realizadas en los últimos seis meses *ha rondado los 50 millones de dólares diarios.* La magnitud del fenómeno empieza a adquirir síntomas de expansión y son cada vez más los que optan por el uso de las *criptodivisas*.

3 OPINIÓN CIBERELCANO:
El Estado Islámico y la Ciberguerra

AUTORES:
Enrique Fojón Chamorro. Subdirector de THIBER, the cybersecurity Think Tank.

(Isis on a hacking / *Baylins.com*)

El pasado 8 de Abril, *la cadena de televisión francesa TV5 Monde sufrió un potente ciberataque* coordinado y perfectamente planificado. Durante varias horas su señal permaneció interrumpida, sus sistemas de información y comunicaciones inutilizados, y los contenidos de su sitio web y sus perfiles en las principales redes sociales virtuales como Twitter o Facebook fueron modificados con mensajes de apoyo al Estado Islámico. Este ciberataque fue reivindicado por el **Cibercalifato**, un grupo de hackers que, afines a la causa del Daesh, ya había reivindicado el pasado enero el *hackeo de las cuentas de Twitter, Youtube y Facebook del Mando Central de las Fuerzas Armadas estadounidenses (USCENTCOM)–* encargado de planear y conducir las operaciones militares de Estados Unidos en Afganistán, Irak y contra Daesh – y del semanario norteamericano *Newsweek*.

A día de hoy, poco sabemos de Cibercalifato: desconocemos su naturaleza, estructura, dependencias, liderazgo –aunque se sospecha que ésta podría estar dirigido por el británico *Junaid Hussain*, condenado en 2012 por comprometer el correo electrónico del Primer Ministro Tony Blair, y huido para combatir junto a Daesh– o zonas desde las que operan. El uso de la denominación ISIS (Estado Islámico de Irak y Siria) y un deficiente árabe en su mensaje reivindicativo del ciberataque contra TV5 Monde ha motivado que muchos analistas pongan en duda su pertenencia al Estado Islámico y lo definan como un movimiento hacktivista pro-Daesh.

No obstante, con independencia de las relaciones que puedan existir entre el Cibercalifato y Daesh, lo cierto es que **a efectos propagandísticos el Estado Islámico asumirá como propios éste y otros ciberataques,** máxime cuando se prevé un *notable aumento en el numero de ataques cibernéticos* –de diferente complejidad e impacto– por parte de grupos afines a la causa del Estado Islámico.

A pesar de que la mayoría de los servicios secretos, fuerzas de seguridad y grandes corporaciones con intereses en las zonas de actuación de las organizaciones terroristas llevan años contemplando como hipótesis de trabajo el uso de cibercapacidades avanzadas por parte de grupos terroristas como al-Qaeda o el Estado Islámico, el ciberataque sufrido por TV5 Monde ha supuesto una importante llamada de atención. La semana pasada, en el marco de la cumbre *Estados Unidos – Consejo de Cooperacióndel Golfo (CCG)* –formado por Bahrein, Kuwait, Omán, Qatar, Arabia Saudita y Emiratos Árabes Unidos– se llegaron a relevantes acuerdos de cooperación en materia de ciberseguridad, especialmente aquellos relacionados con la lucha contra el Estado Islámico en el ciberespacio.

Las principales actividades de las organizaciones terroristas –captación, reclutamiento, adoctrinamiento, adiestramiento, formación o financiación– *se sustentan cada vez más en el uso de las Tecnologías de la Información y las Comunicaciones (TIC)*. Estas organizaciones deben disponer –y disponen– de profesionales TIC de primer nivel para diseñar, securizar y mantener sus infraestructuras informáticas y de comunicaciones. En este sentido, **el Estado Islámico parece estar priorizando la captación de jóvenes europeos con conocimientos y formación en nuevas tecnologías con el objetivo de crear su propio 'ciberejército'.**

No cabe duda de que **el éxito del entramado propagandístico de Daesh se cimienta en el** *carácter viral de las redes sociales virtuales*. Pero para mantener este entramado operativo, éste no sólo dispone de hábiles profesionales de la propaganda y la comunicación en sus filas, sino también de expertos en informática que permitan mantener esta ingente maquinaria propagandística en permanente funcionamiento. Cosa nada fácil porque no sólo implica mantener la operatividad de sus servicios y recursos en línea, en un contexto marcado por continuos cierres y bloqueos de sus cuentas en las redes sociales –*se estima que Twitter ha cerrado hasta 18.000*– y proveedores de servicios, sino también sobreponerse a los múltiples ciberataques que realizan los servicios secretos internacionales o grupos hacktivistas como *Anonymous* contra las redes informáticas y de telecomunicaciones del Estado Islámico.

> "el Estado Islámico también dispone de capacidades de mando y control"

Desde el punto de vista militar, **el Estado Islámico también dispone de capacidades de mando y control** que le permiten dirigir y coordinar sus fuerzas para asestar golpes a los ejércitos iraquí e iraní, tal y como hemos observado a lo largo de los pasados meses. Si asumimos que muchos de estos sistemas de mando y control dependen del ciberespacio para funcionar, requieren una infraestructura TIC para transmitir la información, deben ser seguros y resilientes frente a los ciberataques de

la coalición y tienen que estar permanentemente operativos para poder dirigir la lucha, parece evidente que el Estado Islámico dispone tanto de cibercapacidades –defensivas e inteligencia- como de expertos TIC en sus filas.

Además, es probable que Daesh haya desarrollado capacidades de ciberinteligencia más o menos sofisticadas en línea con las desarrolladas por otros grupos terroristas. Recordemos que Hamas realiza un barrido continuo de las principales redes sociales en *busca de perfiles de soldados de las Fuerzas de Defensa de Israel* para identificar a los soldados y catalogar sus capacidades militares, y que Hezbollah, supuestamente, ha empleado entre los años 2012 y 2015 un *malware de un cierto nivel de sofisticación* para espiar a las empresas de defensa israelíes. En consecuencia, aunque es bien sabido que el Estado Islámico está realizando labores de inteligencia utilizando las redes sociales, no debemos descartar que haya ido un paso más allá y disponga de capacidades más sofisticadas, adquiriendolas en los "bazares de armas ciberneticas" de la dark web.

A falta de conocer si Daesh está en posesión o está desarrollando también capacidades cibernéticas puramente ofensivas, lo cierto es que el hackeo de TV5 Monde debería ser un toque de atención para que los responsables políticos y los expertos constaten **cuáles son las intenciones agresivas de este grupo terrorista en el ciberespacio.** El tiempo nos deparará muchas sorpresas, y no todas positivas.

4 Entrevista a Richard Bach

Assistant Director - Cyber Security. Government's Department For Business, Innovation & Skills. UK.

1. ¿Cuáles son las ciberamenazas de primer nivel que un país desarrollado como Reino Unido tiene que afrontar? ¿Cuál es la naturaleza de las mismas y quiénes son los principales actores tras esas amenazas en el ciberespacio?

Al igual que muchos países de nuestro entorno, el Reino Unido se enfrenta a una amplia gama de amenazas cibernéticas. Si las observamos por nivel de sofisticación, las mayores proceden de otros estados, aunque también de bandas criminales muy bien organizadas; mientras que si lo hacemos en términos de volumen, las amenazas proceden principalmente del crimen organizado y se orientan hacia los ciudadanos y pequeñas empresas.

Posiblemente, los mayores retos a los que nos enfrentamos es la dificultad de detectar y de proteger el país y los ciudadanos frente a las ciberamenzas que acechan.

2. ¿Cuál es la respuesta del Reino Unido ante ese horizonte evolutivo y cambiante de ciberamenazas? ¿Cuáles son las medidas adoptadas por el ejecutivo británico para aportar claridad ante ese panorama confuso y complejo?

Nuestra capacidad de respuesta se ha ido configurando con el paso de los años. Este proceso no es fácil porque la generación de cibercapacidades requiere esfuerzos, tiempo y dinero. De hecho, sin estos tres factores, ni el

Reino Unido ni ningún otro país pueden generar una estructura efectiva y capaz de responder a las amenazas procedentes del ciberespacio.

Además, desde 2011 el Reino Unido dispone de una Estrategia Nacional de Ciberseguridad que no sólo sienta las bases del Programa de Ciberseguridad con un presupuesto de 650 millones de libras para los próximos años, sino también de un Plan de Acción Integral que detalla los objetivos y establece las líneas de acción para lograrlos. De hecho, para su consecución, hemos adoptado un enfoque estratégico que requiere la colaboración de una amplia gama de actores, desde todos los ministerios y agencias del gobierno, alianzas con la industria nacional y el ámbito académico, hasta acuerdos con otros socios como pueden ser la Unión Europea, la Alianza Atlántica o Estados Unidos.

3. Por lo general, los gobiernos regulan su ciberespacio nacional a través de marcos punitivos, en lugar de realizer una definición incentivos o mejores prácticas. ¿Considera que este paradigma punitivo es eficaz o por contra es necesario la creación de un escenario donde la industria considere la resiliencia frente a ciberamenazas como un valor y una inversión y no un coste? ¿Cómo se puede alcanzar estos objetivos y qué mecanismos y factores serían relevantes a tal fin?

Aunque la regulación del ciberespacio es vital, no debemos creer que este escenario funcionará basándose única y exclusivamente en la regulación. La regulación – junto con la imposición de sanciones – del ciberespacio permite normalizar el comportamiento de los actores en este dominio, ya que éstos ni se comportan de la misma manera ni tampoco lo hace igual que en el mundo real. En consecuencia, es necesario establecer un marco regulatorio que permita establecer un código de conducta y un conjunto de buenas prácticas susceptible de alterar el comportamiento de los actores. Dicho de otra forma, el objetivo principal de la regulación no debe ser la compliance sino la cultura.

Por esta razón, aunque en ciertos casos es necesario disponer de un régimen punitivo que acompañe las labores de protección de la información, en ningún caso debería optarse por la sobre-regulación.

Por otro lado, en materia de acciones concretas, debemos tener en cuenta que el Gobierno debe asumir el liderazgo y la coordinación de las actividades. De hecho, la aproximación se realiza siguiendo un esquema de Whole-of-Government approach donde todas las agencias y departamentos del gobierno están implicadas y representadas para reducir los conflictos, coordinar las actividades y facilitar la adopción de medidas concretas, a la vez que se demuestra el compromiso político y la comprensión técnica de todos los actores gubernamentales.

Finalmente, en relación a las actividades a realizar y los mecanismos a generar, probablemente el primer paso es acometer los denominados Cyber-essentials, cinco grandes líneas que permiten comenzar a construir el entramado de ciberseguridad.

4. Teniendo en cuenta su experiencia, ¿hay una necesidad de definir un marco general para la ciberseguridad en España? ¿Cuál es la experiencia del Reino Unido respecto a este aspecto?

En el Reino Unido, cuando pensamos en el marco general para la ciberseguridad, estamos pensando en el esquema de los cyber-essentials. De hecho, éstos proporcionan una descripción básica de los distintos elementos de control de la ciberseguridad y de las medidas de aseguramiento y de confianza necesaria para lograr este control. De hecho, estos elementos son fundamentales para definir, analizar y catalogar las amenazas cibernéticas que se ciernen sobre el país.

"en materia de estructura el gobierno dispone de la National Cyber Crime Agency"

En este sentido, es preciso apuntar que ningún programa integral que tenga medidas más o menos sofisticadas será útil si no se logran los Cyber-essentials. Dicho de otra forma, no sirve de nada que en una casa pongamos puertas blindadas o cerraduras de seguridad si después nos olvidamos la llave en el cerrojo. En consecuencia, es fundamental empezar por la base y, de ahí, ir construyendo el entramado de ciberseguridad nacional. Y para que esto sea posible, es necesario que exista un liderazgo claro y fuerte; y que estos elementos esenciales de la ciberseguridad sean asumidos, integrados y adoptados por todos los actores.

Finalmente, en relación a España, aunque el enfoque de los Cyber-essentials puede tener cabida, solamente los españoles conocen la situación real de su país en relación a los temas cibernéticos ya que España y el Reino Unido no tienen los mismos retos en esta materia.

5. En cuanto a la Estrategia de Ciberseguridad del Reino Unido, ¿cuál es la postura del gobierno británico para hacer frente a la ciberdelincuencia?

Aunque quizás sería necesario describir con detalle lo qué significa cibercrimen, si asumimos la pregunta de forma literal, en materia de estructura el gobierno dispone de la National Cyber Crime Agency – de la que depende la National Cyber Crime Unit – desarrollada a raíz de la Estrategia de Ciberseguridad de 2011. Además, existen numerosas organizaciones regionales y locales que, dependientes de la policía, tienen un importante papel en materia de cibercrimen.

Igualmente, existen acuerdos de colaboración con empresas y otros actores – como puede ser la alcaldía de Londres – para comunicar los incidentes y colaborar en esta materia. Además, también existen otras estructuras fuera de las unidades de cibercrimen, como pueden ser la policía que persigue e investiga a los delincuentes o los CERTs que se dedican a detectar fugas de información.

6. ¿Cuál es el papel del mercado de seguros en relación con la gestión del ciber-riesgo? ¿Estos productos aseguradores se están estableciendo como una estrategia para promover medidas robustas de ciber protección dentro de las empresas?

El papel que el mercado asegurador debe jugar es cada vez más importante. Aunque otros países han empezado a trabajar antes en ello, en el Reino Unido hemos empezado con

fuerza porque consideramos que el mercado asegurador es importante para lograr cambios en el comportamiento de las personas y las empresas. Por lo tanto, desde nuestro país queremos que la población y las organizaciones sean consciente del importante papel que deben jugar los ciberseguros, especialmente en materia de transferencia del riesgo cibernético y de mitigación del mismo.

Por esta razón, desde 2014 estamos trabajando con la industria con el fin de definir las estrategias de mitigación del riesgo. Y, como ya he comentado antes, este elemento se vuelve a relacionar con los Cyber-essentials, como podrían ser en este caso los certificados de cumplimiento o adhesión al esquema de controles mencionado, el alcance de dicha certificación, el papel del tomador de seguros, la política aplicable, etc.

En resumen, el mercado de los ciberseguros es un área emergente con muchos signos positivos y que puede permitir mejorar la cooperación y colaboración entre el gobierno y el tejido empresarial. Creo sinceramente que ello no sólo permitirá incrementar las medidas de ciberprotección – tanto activas como pasivas – de las empresas, sino también el logro de los estándares fijados por el gobierno, puesto que éstos son acreditados y certificados por actores externos e independientes.

7. ¿Existe algún tipo de recompensa para las organizaciones comprometidas con la protección de sus sistemas de información en el Reino Unido? ¿Cómo se reparten los costs entre todos los actores del mercado de la ciberseguridad?

Formalmente no existe ningún premio. Sin embargo, un magnífico premio es que cuanto menos vulnerable sea una organización a los ciberataques, más protegida se halla su propiedad intelectual. Otro "premio" posible es la posibilidad de lograr contratos con el gobierno. Sin embargo, en sentido estricto, no existe ningún reconocimiento concreto para las empresas que cumplan con los estándares; por lo que podríamos concluir que hoy en día el refuerzo consiste en la reducción de los factores negativos más que la existencia de puntos positivos.

En materia de certificaciones, el cumplimiento de los Cyber-essentials es certificable, siendo el coste de certificación básico de 300 libras anuales. No obstante, los certificados avanzados (en función del alcance del ámbito que se le de a la certificación) tienen un coste de más de 1000 libras anuales. Estos certificados permiten demostrar la correcta aplicación de los controles listados en el Cyber-essentials porque cuanto más protegida y segura sea la empresa, es más probable que ésta reciba contratos gubernamentales y, con ello, aumente su nivel de ingresos.

En otras palabras, este modelo es como la ITV de los vehículos, ya que se trata de un examen anual para observar el funcionamiento de la seguridad de la empresa.

5 Informes y análisis sobre ciberseguridad publicados en mayo de 2015

ENCOURAGING THE ADOPTION OF CYBERSECURITY (THIBER e ISMS FORUM SPAIN)

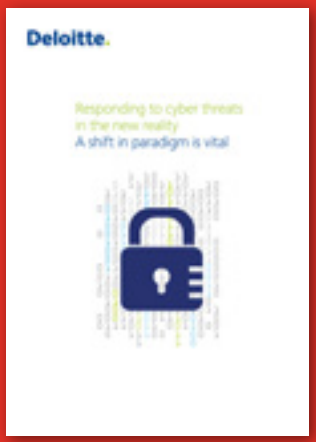
Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks (CCD COE)

WINNING THE CYBERWAR (Deloitte y Symantec)

CERT-UK ANNUAL REPORT (CERT –UK)

U.S Fleet Cyber Command Strategic Plan 2015-2020 (U.S NAVY)

Responding to cyberthreat in the new reality (DELOITTE)



Protocolos y seguridad de red en infraestructuras SCI (INCIBE)

Cyber threats to the Nordic region (Fireeye)

6 Herramientas del analista: MISP (Malware Information Sharing Platform)

El proyecto *MISP (Malware Information Sharing Platform)* es una plataforma opensource de libre descarga desarrollada y mantenida principalmente por el sector de defensa belga y el centro de respuesta a incidentes de la *Agencia de Comunicaciones e Información de la OTAN (NATO NCIA)*.

MISP es una plataforma para compartir, almacenar y correlacionar indicadores de compromisos de ciberataques dirigidos.

Compartir es la clave para una detección rápida y eficaz de los ciberataques. Es bastante frecuente encontrar organizaciones que son objetivo de las mismas campañas de ciberataques, del mismo modo se encuentran similitudes en la tácticas, técnicas y procedimientos (TTPs) empleados por determinados actores que se encuentran detrás de diversas campañas a lo largo del tiempo.

De esta forma, MISP permite compartir información sobre malware y sus indicadores, creando comunidades de intercambio de información sobre amenazas. Los usuarios se benefician del conocimiento colaborativo sobre malware o ciberamenazas ya existentes, implementado mecanismos efectivos de detección y respuesta. Como consecuencia, se reducen de forma significativa los tiempos de respuesta mediante la compartición, el almacenamiento y la correlación de indicadores de compromisos de ataques dirigidos (también conocido como Indicators of Compromise, IoC).

La plataforma por una parte, permite intercambiar información entre analistas a través, por ejemplo, de herramientas de ticketing o notificaciones vía email, comunicando ante nuevos incidentes o indicadores sospechosos. Al mismo tiempo, permite la automatización en la respuesta, permitiendo enviar información a los sistemas de prevención y detección de intrusiones.

La forma de trabajo que implementa MISP permite mejorar el establecimiento de relaciones entre patrones, de forma que cuando se añaden nuevos datos, MISP mostrará de inmediato las relaciones existentes. Esto no sólo permite mejorar el análisis, sino que también permite mejorar las tareas de relación y atribución de los ciberataques.

Entre las principales funcionalidades ofrecidas, MISP permite:

- Crear una base de datos central de Indicadores de Compromiso: almacenando información técnica y no técnica sobre malware y cibertaques y permitiendo importar datos externos en la herramienta.
- Facilidad de uso: es un elemento clave en la plataforma, permitiendo la importación de texto libre, plantillas configurables o datos en formato OpenIOC.
- Correlación: la herramienta estable automáticamente relaciones entre malware, eventos y atributos de ciberataques.
- Seguridad por diseño: MISP es probado regularmente mediante análisis técnicos de vulnerabilidades, incluyendo cifrado PGP y permitiendo firmar digitalmente los emails de alerta entre otras funcionalidades
- Exportación de datos: permitiendo la generación de inteligencia accionable, soportando formatos como STIX (tanto XML como JSON), OpenIOC, texto plano o XML que permite integrarse con otras soluciones de seguridad como IDS o SIEMs
- Importación de datos en formato OpenIOC, sandbox GFI, ThreatConnect, CSV, etc.
- Compartición de datos automáticamente entre otras instancias MISP desplegadas

7 Análisis de los Ciberataques del mes de mayo de 2015

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

Rompiendo con las tendencias de los últimos meses, el mes de mayo de 2015 ha estado caracterizado por una gran actividad maliciosa, tanto en número como en relevancia, cuya materialización principal ha sido los más de nueve grandes casos de fugas de información, afectando a los datos de más de 10 millones de personas en todo el mundo.

CIBERCRIMEN

Entre las principales fugas de información con motivación económica o financiera que se han desarrollado en este periodo, cabe destacar las siguientes:

1. Pacnet, la filial asiática de Telstra que ofrece servicios de centro de datos y de cable submarino, anunció el miércoles 20 de mayo 2015 que fue el blanco de un *ciberataque que supuso la exposición y fuga de datos de miles de usuarios.*

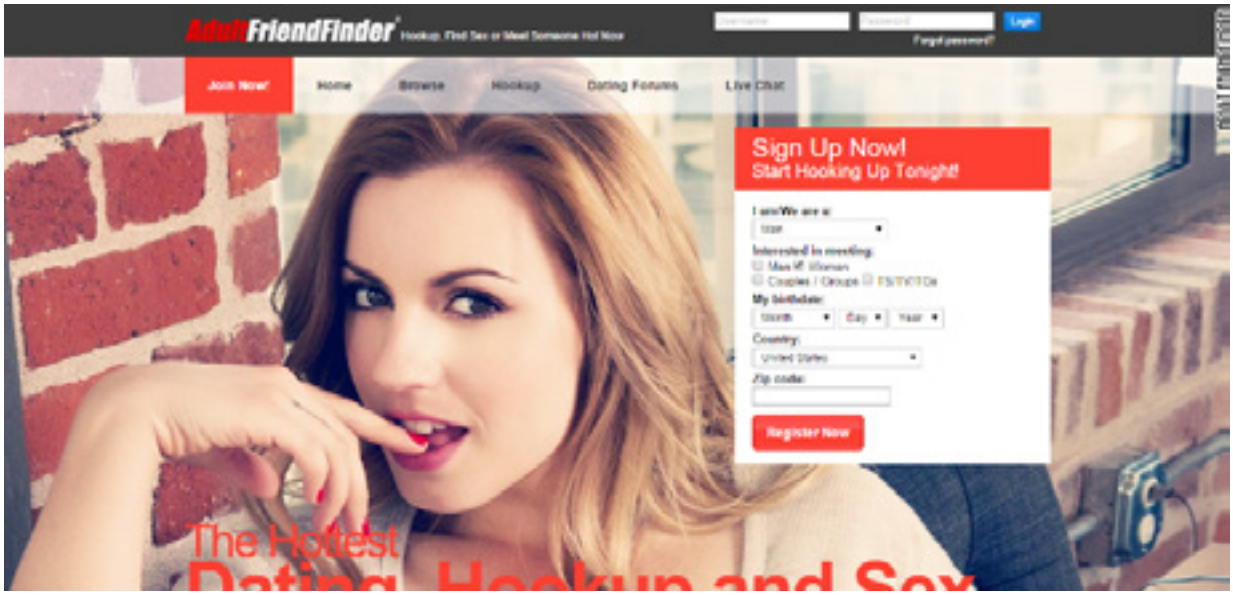
2. En lo que podría ser denominado como el ataque cibernético con más impacto en la historia reciente de Internet de la India, uno de los servicios más populares de streaming de música en ese país, *Gaana.com, fue víctima de un ataque cuya autoría fue reclamada por un hacker pakistaní (Mak Man)* con sede en Lahore, compartiendo un link que permitía ejecutar búsquedas sobre la base de datos de usuarios de todo Gaana.com en su página de Facebook. La fuga de datos afectó a más de 10 millones de usuarios registrados si bien el propio autor comunicaba a través de un *tweet* que no se habían visto expuestos los datos de carácter financiero de los usuarios.

Ilustración 1 BBDD de usuarios extraídos de Gaana.com

3. Tras las oleadas de ciberataques sufridas por el sector asegurador en lo que llevamos de año, esta vez ha sido *CareFirst BlueCross BlueShield la entidad afectada.* Los atacantes tuvieron acceso a la base de datos central de la organización, exponiendo los datos de más de 1,1 millones de asegurados.

Ilustración 2 Comunicado publicado por CareFirst

4. El pasado jueves 21 de mayo, 3.9 millones de datos de usuarios de la web de citas para adultos *AdultFriendFinder fueron publicados.* Entre los datos que han visto la luz, se encuentran preferencias sexuales, fetichismos y otra suerte de datos personales de los usuarios, como email, dirección o el código postal. El atacante trató de extorsionar a la web de citas solicitando el pago de 100.000 dólares a fin de no publicar los datos robados. Adicionalmente ha amenazado con realizar ataques dirigidos a los usuarios empleado los datos sustraídos.



5. A mediados de mes, se publicó en un foro en la Dark Web de la *base de datos de los más de 400.000 usuarios* potenciales de *mSpy* una empresa que comercializa un software de para espiar dispositivos móviles.

6. El *Internal Revenue Service (IRS)* norteamericano fue víctima de un ataque dirigido mediante el cual diversos atacantes, a través de un servicio web ofrecido por el propio IRS, accedieron a la información personal relativa los impuestos de más de 100.000 contribuyentes, formando parte de un elaborado plan de robo de identidades para reclamar la devolución de impuestos de forma fraudulenta.

7. La *Oficina de Administración de Personal (OPM)* de la administración estadounidense se ha convertido en la última víctima de una gran fuga de información que ha afectado a los datos de más de 4 millones de empleados federales. Las pesquisas iniciales realizadas tras el incidente por parte del US-CERT del Departamento de Homeland Security norteamericano y el FBI, los informes iniciales apuntan a China como presunto autor material de los ciberataques. Las consecuencias aun están por determinar, pero la preocupación de la Administración estadounidense sobre entidades como la OPM va en aumento. Estos grandes procesadores de datos públicos se han convertido en objetivo recurrente de ciberataques, ya que la OPM fue *atacada también en el periodo estival de 2014, viéndose afectados miles de datos de empleados públicos que habían aplicado para obtener la acreditación de seguridad Top-Secret.*

8. El *sistema de pensiones públicas japonés ha sido víctima de un ataque dirigido mediante un malware distribuido mediante técnicas de spearphising.* Como resultado, los nombres y números de la seguridad social japonesa de 31000 personas así como los nombres y fechas de nacimiento de otros 1,25 millones de japoneses se han visto comprometidos. Asimismo, los nombres y direcciones de otros 50.000 ciudadanos también se vieron afectados. Este ataque se produce tan sólo unos días después del anuncio realizado por Estados Unidos relativo a la extensión de sus "líneas de defensas cibernética" a Japón en un esfuerzo para ayudar a proteger a su aliado asiático contra el creciente número de ciberataques a redes militares y a las infraestructura críticas del país nipón.

Junto con estas grandes fugas de información, en mayo se ha experimentado un repunte de los ciberataques sobre el sector retail a nivel mundial. En los dos últimos años, ha habido una proliferación de malware específicamente diseñado para extraer información de las tarjetas de crédito del Punto de Venta (POS por sus siglas en inglés-). En 2015, ya han aparecido variedades de malware nuevo para POS incluyendo nuevas variantes y cepas de *Alina*, *LogPOS*, *FighterPOS* y *Punkey*. La firma FireEye ha publicado una nueva investigación en una amplia campaña de spam focalizada en la distribución de malware para POS, que han denominado *NitlovePOS*.

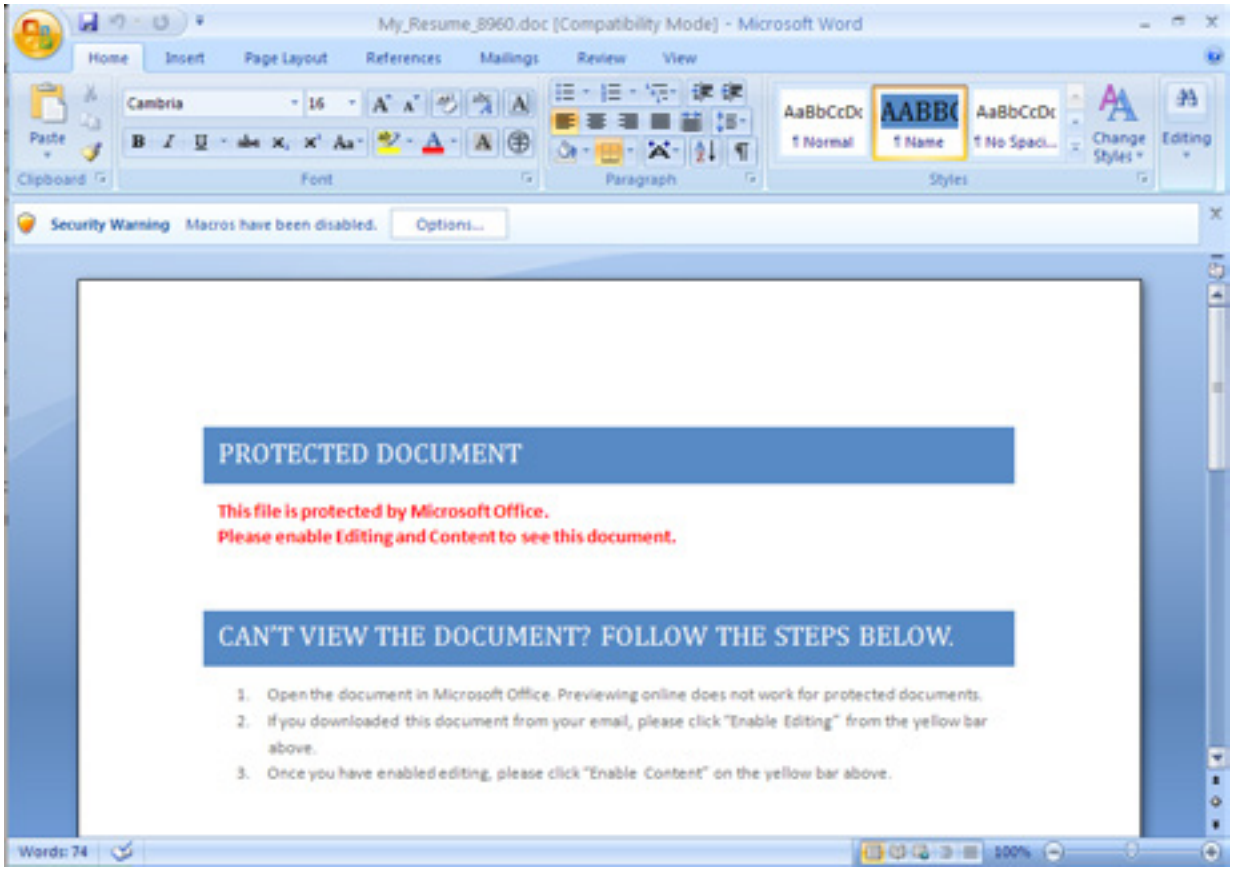


Ilustración 3 Documento con la macro maliciosa que se recibe como adjunto a un email en la campaña NitlovePOS

CIBERESPIONAJE

Durante este mes, las principales campañas de ciberespionaje han estado aparentemente patrocinadas y ejecutadas por actores pro-rusos, tanto estatales como no estatales.

La *Operación Armageddon*, investigada y recientemente detectada por la firma Lookingglass Cyber Solutions, ha estado activa desde mediados de 2013, siendo su foco principal los entes gubernamentales, militares y fuerzas y cuerpos de seguridad del estado ucraniano. Si bien no es nuevo este tipo de campañas (conviene recordar la campaña *Ouroboros* de marzo de este año), el momento temporal en el cual tuvo lugar el inicio de la campaña sugiere que el comienzo debió ser motivado por la decisión de Ucrania de aceptar el Acuerdo de Asociación entre Ucrania y la Unión Europea (AA), diseñado para mejorar las integraciones económicas entre ambos mercados. Los líderes rusos interpretaron públicamente este movimiento por parte de Ucrania como una amenaza para la seguridad nacional rusa. Aunque los primeros pasos para adherirse a la AA ocurrió en marzo de 2012, la campaña no comenzó hasta casi un año más tarde (mediados de 2013), coincidiendo con la cristalización del acuerdo entre Ucrania y la UE.

Por otra parte, el departamento TIC del Bundestag alemán, fue víctima de un sofisticado ataque dirigido sobre sus redes internas, el pasado 15 de mayo, tal y como informaba *Der Spiegel*. También en este caso, un grupo de hackers pro-rusos con base en Ucrania han reclamado la responsabilidad del ataque.

Por otra parte, los analistas de ClearSky han descubierto una campaña de ciberespionaje en Oriente Medio llamado *Thamar Reservoir* debido al nombre de su objetivo Thamar E. Gindin. Los atacantes centraron sus esfuerzos en conseguir acceso remoto sobre las máquinas de la víctima para hacerse con el control las cuentas de correo electrónico asociadas. Aparentemente no hay evidencias de motivaciones financieras, circunstancia que sugiere la implicación de los actores estatales.

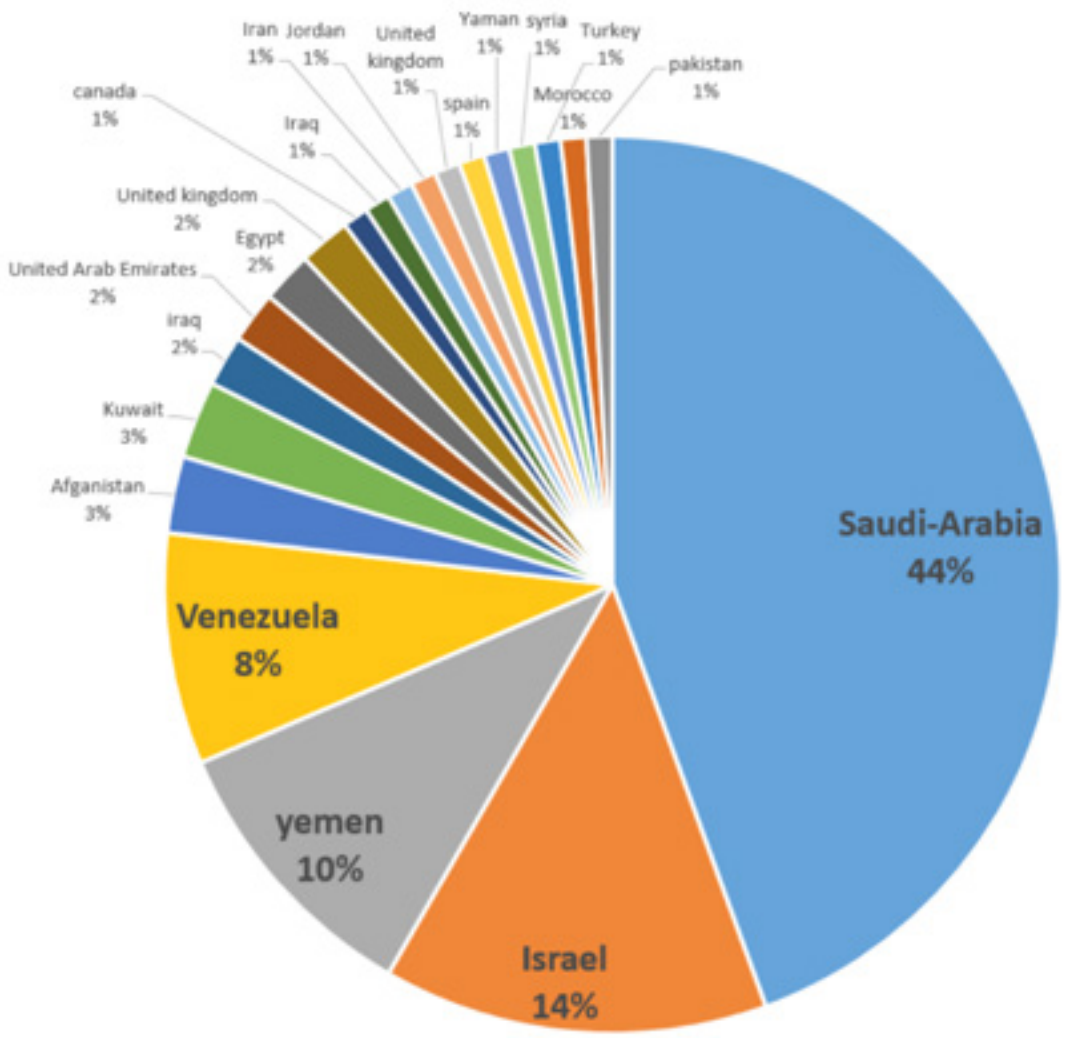


Ilustración 4 Distribución de las víctimas de la campaña de ciberespionaje Thamar Reservoir

HACKTIVISMO

En cuanto a las motivaciones políticas y activistas, el mes de mayo ha estado marcado por el retorno del Ejército Sirio Electrónico (SEA), que ha *atacado, una vez más, el Washington Post*, realizando una redirección hacia una web controlada por el SEA.

Por otra parte, miembros del movimiento hacktivista Anonymous lograron extraer información, a través de ataques de inyección SQL, de las *bases de datos de la Organización Mundial del Comercio (OMC)*. Como consecuencia, los datos de más de 2000 empleados de la OMC han sido publicados en diversas webs de intercambio de datos.

Anonymous Italia continúa apuntando a la Expo 2015, que actualmente se está celebrando en Milán, con una serie de ataques dirigidos contra los sistemas y las redes de las empresas que están trabajando en la coordinación del evento.

La última víctima de la operación *#OpItaly* ha sido Best Union, una empresa que gestiona el servicio de venta de entradas online, realizando un ataque de DDoS y de defacement de su web.

Ilustración 5 Defacement de la web http://padiglioneitaliaexpo2015.com/

El pasado 20 de mayo, el grupo autodenominado como Yemen Cyber Army (YCA) ha lanzado un *ataque dirigido contra los sistemas informáticos en Arabia Saudí*, principalmente contra los servidores web y las bases de datos del Ministerio del Interior y del Ministerio de Defensa. El YCA ha publicado más de un millón de documentos confidenciales y de planificación estratégica gubernamental. Los datos incluyen también mensajes de correo electrónico, información personal y secretos de estado del personal del Gobierno y diplomáticos que han participado en diferentes misiones en todo el mundo.

Ilustración 6 Defacement realizado por el YCA sobre diversas webs gubernamentales saudíes

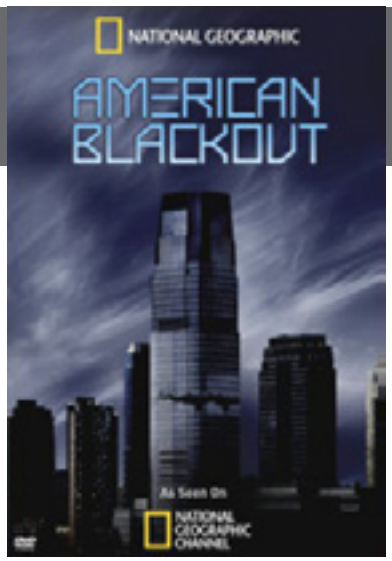
Además, el grupo afirmó que ha tenido acceso a la red del Ministerio de Asuntos Exteriores (MOFA), pero afirman al mismo tiempo controlar un total de 3.000 ordenadores y servidores, así como miles de usuarios.

Los ataques se engloban dentro una protesta contra los ataques saudíes sobre territorio yemení. El YCA ha anunciado la publicación de un millón de documentos semanalmente, entre ellos los datos de los visados sustraídos, hasta que no finalicen los ataques, habiendo enviado más de medio millón de documentos confidenciales (unos 30 GB) a Wikileaks.org para que actúen como backup de la información.

La web *www.databreaches.net* ha publicado un análisis detallado del contenido de la base de datos publicado por el YCA.

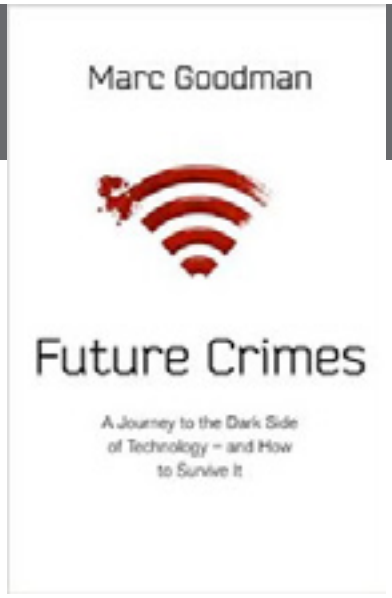
8 Recomendaciones

8.1 Libros y películas



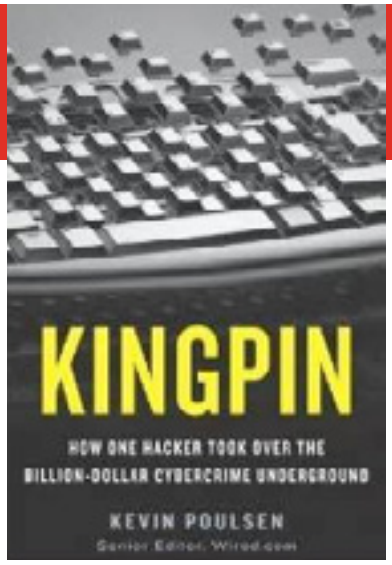
Película:
AMERICAN BLACKOUT 2013

National Geographic recrea los catastróficos efectos que podría ocasionar un ciberataque coordinado, duradero y a gran escala contra la red eléctrica de los Estados unidos



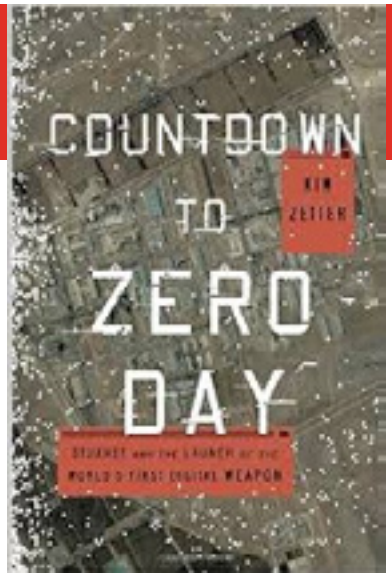
Libro:
FUTURE CRIMES

Autor: Marc Goodman
Num. Paginas: 464
Editorial: Bantam Press
Año: 2015
Precio: 18.00 Euros
Sinopsis: El autor realiza, tras un extenso repaso histórico, un análisis prospectivo del uso de las nuevas tecnologías por parte de las bandas de cibercriminales.



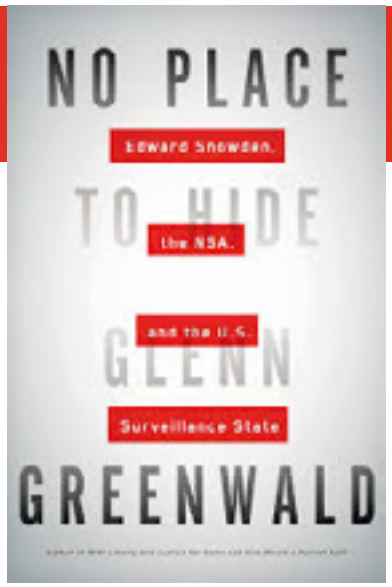
Libro:
KINGPIN

Autor: Kevin Poulsen
Num. Paginas: 289
Editorial: Crown
Año: 2011
Precio: 12.00 Euros
Sinopsis: Kevin Poulsen, un reputado periodista tecnológico, nos presenta una historia en la que se esbozan las futuras tendencias del cibercrimen.



Libro:
COUNTDOWN TO ZERO DAY

Autor: Kim Zetter
Num. Paginas: 448
Editorial: Crown
Año: 2014
Precio: 13.00 Euros
Sinopsis: Kim Zetter, un reputado periodista en el campo de la ciberseguridad, narra la historia completa del gusano Stuxnet y como este fue utilizado para menoscabar el programa nuclear iraní.



Libro:
NO PLACE TO HIDE

Autor: Glenn Greenwald
Num. Paginas: 264
Editorial: Penguin
Año: 2014
Precio: 9.00 Euros
Sinopsis: Glenn Greenwald realiza un repaso por los principales documentos filtrados por el ex contratista de la NSA Edward Snowden.

8.2 Webs recomendadas

http://www.wired.com/category/security
WIRED dispone de una sección específica donde se tratan las principales noticias en materia de ciberseguridad.

https://www.europol.europa.eu/ec3
Sitio web del European Cybercrimen Centre (EC3) de la Europol.

https://www.acsc.gov.au/
Sitio web del Centro de Ciberseguridad del gobierno australiano. Es especialmente relevante su área de publicaciones.

http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-CyberlawTracker.aspx
La UNCTAD dispone de una base de datos interactiva con las legislaciones en materia ciber de la inmensa mayoría de los planetas del globo.

https://www.rsaconference.com/
Sitio web de la conferencia RSA. Especialmente relevante su sección de Blogs donde los principales expertos en ciberseguridad comparten sus opiniones y experiencias.

http://www.cyberessentials.org/
Sitio web de Cyberessential, una de las iniciativas del gobierno británico para el fomento de la seguridad en el ciberespacio entre las empresas británicas.

8.3 Cuentas de Twitter

@criptored

@EFF

@Red_Seguridad

@GDTGuardiaCivil

@osiseguridad

9 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
1-2 junio	Lisboa	ISEG Lisbon	2015 European Security Conference: Security in the Internet of Things	http://secconf.iseg.ulisboa.pt/
1-5 junio	Queensland, Australia	AusCERT	AusCERT2015: Smarten up	https://conference.auscert.org.au/
2-3 junio	Fort Meade, Maryland	NSA	NSA SIGINT Development Conference 2015	https://www.fbcinc.com/event.aspx/Q6UJ9A010V27
42158	Londres	Security B-Sides	BSides London	https://www.securitybsides.org.uk/
2-4 junio	Londres	InfoSecurity Europe	InfoSecurity Europe 2015	http://www.infosecurityeurope.com/
2-3 junio	Buenos Aires	Centro de Ciberseguridad Industrial	IV Congreso Internacional de Ciberseguridad Industrial	https://www.cci-es.org/web/cci/detalle-congreso/-/journal_content/56/10694/135953
2-3 junio	Nueva York	Office of Information Technology Service. New York State	18th New York State Cyber Security Conference	https://its.ny.gov/annual-cyber-security-conference-june-2-3-2015
6-10 junio	Shenyang, China	IEEE	IEEE Cyber	http://www.ieee-cyber.org/2015/
8-9 junio	Londres	C-MRiC	International Conference On Cyber Situational Awareness, Data Analytics And Assessment	http://c-mric.org/index.php/csa-2015home

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
11 junio	Copenague	Ministry of Business and Growth. Denmark	Copenhagen CyberCrime Conference 2015	http://cccc-2015.com/
11 junio	Madrid	Red Seguridad	VII Encuentro Integral de la Seguridad (Seg2)	http://www.redseguridad.com/revistas/red/eventos/seg2_VII/seg2_VII_programa.pdf
14-19 junio	Berlin	FIRST	Annual FIRST Conference	http://www.first.org/conference/2015
16-18 junio	Londres	Black Hat	Black Hat Mobile Security Summit	http://blackhat.com/ldn-15/
17-18 junio	Cardiff	Nuclear Energy Insider	Nuclear Knowledge Management and Cyber Security	http://www.nuclearenergyinsider.com/cyber-security/
20-21 junio	Paris	hackerzvoice	Nuit du Hack 2015	https://www.nuitduhack.com/en/
22-23 junio	Delft	National Cybersecurity Centrum. The Netherlands	14th Annual Workshop on the Economic of Information Security (WEIS 2015)	http://weis2015.econinfosec.org/
23-24 junio	Tel Aviv	Prime Minister's office National Cyber Bureau	Cybersecurity Conference 2015	http://sectech.tau.ac.il/cyberconference15/
29-junio	Washington	NSA	NSA Information Assurance Symposium (IAS) 2015	http://www.fbcinc.com/event.aspx/Q6UJ9A010TUN

REAL INSTITUTO
elcano
ROYAL INSTITUTE

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