MARZO 2016 / Nº 12

CIBER elcano

Desarrollado por:

INFORME MENSUAL DE CIBERSEGURIDAD

Copyright y derechos:

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

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

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

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

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

Informe editado en Madrid.

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank.

Índice

1 Comentario Ciberelcano 04

2 Análisis de actualidad internacional 06

3 Entrevista a Carles Solé.....10

4 Informes y análisis sobre ciberseguridad publicados en febrero de 2016 13

5 Herramientas del analista 14

6 Análisis de los ciberataques del mes de febrero de 2016 15

7 Recomendaciones

7.1 Libros y películas 20

7.2 Webs recomendadas 22

7.3 Cuentas de Twitter.....22

8 Eventos.....23

1 COMENTARIO CIBERELCANO
En busca de la superioridad tecnológica

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

La obligada necesidad del Departamento de Defensa (DoD) estadounidense por estar en la vanguardia de la innovación tecnológica – como elemento central de *la Tercera Estrategia de Compensación (Third Offset Strategy)* lanzada por el exsecretario de Defensa Chuck Hagel a finales de 2014 – condicionó la elaboración de su nueva estrategia cibernética, presentada ya por el actual titular del Pentágono Ashton Carter en Abril de 2015.

Más allá de las líneas maestras establecidas en materia estratégico-militar por la nueva estrategia cibernética del Pentágono, el elemento más relevante es que el DoD ha descubierto que el primer – y quizás el único – paso para seguir manteniendo la supremacía militar y seguir siendo la primera potencia mundial en materia cibernética pasa por dinamizar, potenciar y consolidar la industria nacional de ciberseguridad.

Desde que comenzó su mandato en Febrero del pasado año, Carter ha intensificado sus visitas a Silicon Valley, epicentro mundial de la innovación tecnológica. La última visita se producía hace tan solo unos días con el objetivo de reunirse con los dirigentes de las principales empresas tecnológicas del país – en el marco de la prestigiosa *RSA Conference* sobre criptografía y seguridad de la información – y promover la recientemente creada *Defense Innovation Unit Experimental (DIUx).*

La DIUx fue creada en Julio de 2015 en el marco de la *Defense Innovation Initiative* para generar nuevas capacidades militares y el *Long Range Research and Development Plan*

para apoyar las propuestas tecnológicas de la industria civil estadounidense para madurarlas e integrarlas en los sistemas armamentísticos claves para la Tercera Estrategia de Compensación. En este sentido, Carter explicó que *"el DoD quiere colaborar con todas las empresas innovadoras del país . Por tanto, si vamos a aprovechar las nuevas tecnologías, el Departamento de Defensa debe trabajar conjuntamente junto a los innovadores".* Localizada en Silicon Valley, el DIUX actúa como embajada del DoD con el objetivo principal de identificar aquellas tecnologías emergentes que permitan mantener la superioridad tecnológica del Pentágono, posibilitando así mantener la condición de primera potencia mundial. Del mismo modo, la veintena de miembros –civiles y militares – del DIUx deberán afianzar la relación con los contratistas tradicionales del DoD y como explicó el secretario de defensa deberá *"familiarizar a una nueva generación con la misión de seguridad nacional, haciéndoles partícipes de ella si así lo desean."*. En la actualidad, debido al carácter experimental del DIUx, esta trabaja con un conjunto reducido de start-ups con un alto grado de innovación, sin perder de vista el estado del arte del mundo tecnológico.

En definitiva, con iniciativas como el DIUx, el Departamento de Defensa y sus Fuerzas Armadas pretenden disponer de los medios, capacidades y conocimientos necesarios para mantener el liderazgo tecnológico, especialmente el relacionado con el ciberespacio. La mayoría de estos avances no proceden de la industria militar sino de la civil, y es por ello que todos los planes de desarrollo de nuevas capacidades militares vinculados con la Tercera Estrategia de Compensación – y en particular el DIUx en materia de cibercapacidades – se basan en la colaboración público-privada. Muchas lecciones deberíamos de aprender de estas iniciativas.

"el DIUX actúa como embajada del DoD con el objetivo principal de identificar aquellas tecnologías emergentes que permitan mantener la superioridad tecnológica del Pentágono"

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
Jornadas de Ciberdefensa 2016
"Operaciones Militares en el Ciberespacio"

AUTOR: GD. Carlos Gómez López de Medina. Comandante Jefe del Mando Conjunto de Ciberdefensa (MCCD)

Con frecuencia se confunden o utilizan indistintamente los términos **ciberseguridad y ciberdefensa.** Este artículo trata de lo segundo, la **ciberdefensa** como componente específico y distintivo de la ciberseguridad por su naturaleza eminentemente **militar**, y expone la oportunidad de la celebración de unas **Jornadas específicas de Ciberdefensa,** aglutinadoras de todos los aspectos de las Operaciones Militares en el Ciberespacio.

De una forma muy simple, podríamos definir la ciberdefensa como el conjunto de acciones, medios y procedimientos para asegurar el uso propio del ciberespacio y negarlo al enemigo. El **ciberespacio** ha sido objeto de confrontación, de forma más o menos soterrada, desde principios de la década de los noventa, hasta el punto que podemos decir que en la mayoría de conflictos armados acontecidos en los últimos veinte años también se ha combatido, de manera incremental, en el ciberespacio. No resulta descabellado suponer que prácticamente la totalidad de los conflictos venideros se iniciarán, e incluso finalizarán, en él.

Podemos definir **ciberguerra** como el conflicto bélico que utiliza el ciberespacio como escenario principal, en lugar de los campos de batalla convencionales. El ciberespacio tiene características únicas, de las que por su incidencia en el ámbito de la Defensa destacamos su carácter transversal, la indefinición legal y ausencia de normativa común, la tremenda dependencia y escasa concienciación, la diversidad de actores y fragmentación en las responsabilidades, la compleja superficie a defender y lo impredecible del alcance de los ataques, las dificultades en la atribución y en la capacidad de disuasión efectiva, la volatilidad tecnológica, la inexistencia de un control de "ciberarmamento" o la difícil gestión de las crisis en el ciberespacio.

Las características anteriores, unido a la accesibilidad del ciberespacio, lo convierten actualmente en el "terreno" idóneo para las

denominadas **guerra de la información y operaciones de influencia.** Si a ello se agrega el relativamente bajo coste de las acciones y los elevados daños potenciales al adversario, es fácilmente comprensible que la ciberguerra sea el **paradigma de la guerra asimétrica** que tanto ha desestabilizado el status-quo existente hasta finales del siglo XX. Si las operaciones militares tradicionales siempre se han medido en parámetros de distancia y tiempo, la inmediatez y ubicuidad del ciberespacio lo han consagrado de facto como el **quinto dominio de la guerra,** transversal y distintivo de los cuatro precedentes, tierra, mar, aire y espacio. La posibilidad de anonimato, las dificultades en la atribución y localización certeras de las acciones y la presencia cotidiana de múltiples actores (hackers, hacktivistas, ciberdelincuentes, ciberterroristas, etc) convierte también al ciberespacio en un vector principal de la **guerra híbrida.**

"El ciberespacio es el quinto dominio de las operaciones militares. La ciberguerra es el paradigma de la guerra asimétrica y vector de la guerra híbrida"

En la actualidad, la práctica totalidad de naciones avanzadas ya cuentan con unidades especializadas para operar en el quinto dominio. Por regla general, el ámbito de actuación de estas unidades son las **redes y sistemas militares,** aunque en algunos casos o circunstancias se amplía a sistemas relacionados con **infraestructuras críticas** o incluso en la **lucha antiterrorista.** Si bien su actividad se enfoca prioritariamente hacia la **defensa,** sus capacidades suelen abarcar también la **ciberinteligencia** y las **operaciones ofensivas.**

En este complejo entorno opera cada día el **Mando Conjunto de Ciberdefensa (MCCD)** desde su creación en 2013. Entre los cometidos del MCCD está, al igual que se hace con los espacios aéreos y marítimos de soberanía, la **vigilancia permanente** del ciberespacio, garantizando el libre acceso y la disponibilidad, integridad y confidencialidad de la información y de las redes y sistemas de su responsabilidad. El MCCD tiene encomendado obtener, analizar y explotar la **información sobre ciberataques e incidentes** en esas mismas redes y sistemas, y ejercer en su caso la **respuesta** oportuna, legítima y proporcionada en el ciberespacio **ante amenazas o agresiones** que puedan afectar a la **Defensa Nacional.** Estos tres cometidos determinan sus ámbitos de actividad en el plano operativo **-defensa, explotación y respuesta-** como un componente más de la **Fuerza Conjunta.**

Además, corresponde al MCCD ejercer la **representación** del Ministerio de Defensa en el ámbito **nacional e internacional**, así como definir, dirigir y coordinar la **concienciación**, la **formación** y el **adiestramiento** especializado en materia de ciberdefensa.

Quizás uno de los ingredientes esenciales para asumir los cometidos asignados al MCCD, mitigar los innumerables riesgos que presenta el ciberespacio y aprovechar también sus múltiples oportunidades ha sido la **cooperación**.

La **cooperación**, identificada como factor clave en la Estrategia Nacional de Ciberseguridad, es una de las **señas de identidad del MCCD** desde el mismo momento de su creación. Cooperación no sólo en el ámbito interno del Ministerio de Defensa, sino también, en su dimensión **nacional e internacional**, con **organismos públicos y privados, empresas, investigadores y universidades.** En los tres años de vida del MCCD que acabamos de celebrar hemos constatado cómo ese espíritu de cooperación y mentalidad colaborativa ha propiciado el aumento de capacidades y la sinergia de voluntades y esfuerzos de todos los actores implicados, permitiéndonos alcanzar importantes hitos colectivos.

Por todo lo anterior, como foro de exposición y debate del **estado del arte** en todas las dimensiones de la ciberseguridad, entorno para la **puesta en común** de esos logros y también como plataforma de **conocimiento y relación** a nivel nacional e internacional, que posibilite nuevas **oportunidades de cooperación** y convergencia, el MCCD organizará las **Jornadas de Ciberdefensa 2016 "Operaciones Militares en el Ciberespacio"** entre los días **23 y 26 de mayo en Kinépolis Madrid (Ciudad de la Imagen).** Se trata de las segundas desde su creación, tras las del 2014.

Se trata de una ocasión sin precedentes en este ámbito. Las Jornadas pretenden explorar las **técnicas, tácticas y procedimientos** que se están utilizando en las operaciones militares en el ciberespacio. Se compartirán experiencias y **lecciones aprendidas de operaciones recientes** a nivel nacional e internacional, como por ejemplo los ataques más sofisticados del tipo "amenazas persistentes avanzadas" o **APT´s** (Advanced Persistent Threats). También se abordará cómo afrontar el reto de la integración de la ciberdefensa en el **proceso de planeamiento operativo,** a fin de alcanzar un nivel adecuado de coordinación y sincronización con el resto de acciones militares convencionales y de influencia.

El papel de la ciberdefensa ante el potencial impacto en la Seguridad Nacional de ataques a **operadores e infraestructuras críticos** constituirá otro punto destacado de la agenda, para lo que se contará con destacados ponentes del sector.

Las Jornadas dedicarán una atención especial a los **aspectos legales** del ciberespacio. La próxima publicación de la segunda edición del Manual de Tallinn sobre Derecho Internacional Aplicable a la Ciberguerra **(Manual de Tallinn 2.0)** permitirá la exposición y debate por prestigiosos juristas sobre lo último en restricciones legales y **reglas de enfrentamiento** aplicables a operaciones de ciberdefensa. Igualmente, representantes de las principales organizaciones de seguridad y defensa a nivel internacional y

nacional abordarán su **dimensión estratégica** y proporcionarán una visión actualizada del estado de las principales **iniciativas, normas y proyectos.**

Si la cooperación es fundamental para la defensa y la explotación de los propios intereses en el ciberespacio, lo es más si cabe para su configuración futura. El MCCD dedica una parte importante de sus esfuerzos a la colaboración con la **industria** y con la **universidad** para fomentar **la investigación, el desarrollo y la innovación,** así como la **formación** avanzada en ciberseguridad. Esta colaboración se materializa en la presencia del Mando en diversos **proyectos** a nivel internacional y nacional, y su participación en numerosos **convenios de carácter tecnológico y docente,** que también se expondrán en las Jornadas. La universidad, como no podía ser menos, también estará presente en las Jornadas del mes de mayo.

Por último, el grado de operatividad del MCCD y de las Fuerzas de Ciberdefensa no sería posible sin la inestimable participación de la industria, capacitador y puntal con sus desarrollos de la investigación e innovación necesarios para disponer de **ventaja competitiva** en un dominio tan dinámico como el del ciberespacio. Las **principales empresas del sector** tendrán una participación destacada en las Jornadas, presentando y promocionando sus soluciones y brindando su patrocinio.

En las Jornadas se darán cita destacados representantes de la ciberdefensa a nivel mundial. Citar como ejemplos las principales **naciones de Iberoamérica** y de la **Iniciativa 5+5** -que integra a los países de las costas sur de Europa y norte de África-. Con todos ellos compartimos siglos de historia y cultura, intereses comunes y, en muchos casos, robustas relaciones bilaterales. Las Jornadas constituirán por lo tanto un foro privilegiado para el conocimiento mutuo y establecimiento de relaciones.

Las Jornadas de ciberdefensa se enmarcan en las actividades previas a la celebración del **Día de las Fuerzas Armadas**, poniendo de manifiesto la voluntad y vocación participativa de la Defensa Nacional para el bien común. Por lo tanto, agradeciendo la oportunidad que nos brinda esta prestigiosa tribuna, aprovechamos para invitarles a participar en estas, sus Jornadas de Ciberdefensa, de las que en próximas ediciones ampliaremos información.

Jornadas de Ciberdefensa 2016 del Mando Conjunto de Ciberdefensa
“Operaciones Militares en el Ciberespacio”
Kinépolis Madrid
(Ciudad de la Imagen, Pozuelo de Alarcón)
23 al 26 de mayo de 2016
www.jornadasciberdefensa2016.es

3 Entrevista a Carles Solé.

Director de Seguridad de la Información CaixaBank, MBA, CISM, CGEIT, CRISC, CISSP

1. Como responsable de seguridad de la información de CaixaBank, ¿podría indicarnos cuáles son las principales competencias dentro de su área? ¿Cuál es su rol en la implementación de la estrategia corporativa?

Desde el departamento lideramos tanto el diseño como la implementación de la estrategia corporativa en materia de seguridad de la información. Para garantizar las diferentes facetas de la misma tenemos organizado el departamento en tres áreas: (1) gobierno de la seguridad, que analiza los riesgos, establece las políticas y vela por su cumplimiento, además de trasladar los diferentes requisitos regulatorios a las mismas; (2) protección de la información, que diseña e implementa los procesos y los proyectos orientados a mitigar los riesgos, además de liderar la labor de concienciación en materia de seguridad a toda la organización; y (3) ciberseguridad, que diseña la estrategia y pone los medios para hacer frente a las ciberamenazas, apoyado por nuestro equipo de Cyber Security Response Team.

2. ¿Cuáles son las amenazas de seguridad a las que se encuentra expuesta una entidad bancaria como CaixaBank? ¿Están focalizadas contra sus propios activos digitales o contra sus clientes?

Por un lado, continúan las tradicionales en el sector bancario, focalizadas en explotar las debilidades de nuestros clientes (phishing, troyanos bancarios) Siguen y seguirán estando

presentes, pues se basan en el engaño y en las innumerables formas de vulnerar los sistemas operativos y las aplicaciones.

Pero, en los últimos años, la amenaza de los APTs y, más recientemente, de los ransomware se están haciendo patentes. El foco en las fortalezas de nuestros activos digitales resulta esencial. Lo vimos venir y hemos desplegado un buen ecosistema de defensa, pero la complejidad creciente de dichas amenazas hace que no podamos dejar de evolucionar ni un sólo instante.

3. El intercambio de información sobre ciberamenazas en el sector bancario es y ha sido objeto de debate, por la madurez del propio sector y por el nivel de exposición del mismo ¿podría explicarnos cómo se articula ese intercambio de información de amenazas y ciberinteligencia? ¿se realiza de forma bilateral con otras entidades o bien a través de algún agente nacional o internacional (tipo FS-ISAC)?

Pues después de muchos años buscando buscando la forma efectiva de intercambio, algo que nos hubiese facilitado mucho la lucha contra el cibercrimen, empezamos por fin a tener los canales adecuados a nuestra disposición. FS-ISAC es uno más, cierto que particular del sector bancario, pero también nos interesa y mucho el intercambio de amenazas y campañas a nivel nacional, por la particularidad de las mismas. Aquí las herramientas son lo de menos, lo relevante es que los actores que participen en estas redes de intercambio aporten información relevante. Y que dicha información seamos capaces de procesarla y accionarla de la forma más automatizada posible.

4. Respecto a los formatos de intercambio de información de amenazas (STIX, TAXII, Cybox, OpenIoC, etc.) ¿cuál considera que es la estrategia a seguir por el sector? ¿Adopción de dichos estándares? ¿creación de un formato propio?

Debe existir un formato estándar para el intercambio con terceros, ya sea del propio sector, multisectorial o de agentes nacionales/internacionales. De otro modo no tendría sentido. Nuestra visión es la adopción de los modelos y herramientas que mejor se ajusten a nuestra realidad interna, pero con conectores y orquestadores capaces de comunicarse a través de estándares con el resto de entidades e instituciones que nos puedan aportar información útil para nuestras defensas.

5. Bajo la óptica de una entidad financiera, ¿qué medidas de control o de coordinación echa en falta por parte de la Administración con el objetivo de mejorar la respuesta ante ciberincidentes?

Empiezan a surgir, por fin, algunas iniciativas para el intercambio de información sobre los indicadores de compromiso que caracterizan

a las mismas. Pero aún queda recorrido para llegar a un escenario maduro que permita ese intercambio de forma global y eficiente.

Y hay algo que llevamos repitiendo desde hace años desde el sector privado, y es la necesidad de actuar de forma efectiva contra los cibercriminales. Tenemos capacidad para detectar y defender nuestros activos contra este tipo de amenazas, tenemos información que permitiría iniciar procesos contra los que las perpetran. Pero los cauces para denunciar y llevar a cabo dichas acciones son, todavía, insuficientes.

6. Con la proliferación del concepto de omnicanalidad, los servicios financieros se han vuelto más globales, móviles, digitales y basados en la nube. ¿Qué significan estas tendencias desde el punto de vista de la ciberseguridad y la gestión de riesgos tecnológicos para el sector financiero?

Significan un cambio de paradigma en el modo de abordar la ciberseguridad. De un modelo basado en el control casi absoluto de los activos digitales a otro en el que dichos activos están bajo la responsabilidad de un tercero, ya sean empresas proveedoras de servicios cloud o de entornos gobernados casi por completo por los usuarios (BYOD y similares) Las estrategias basadas en controlar y bloquear van a ir en detrimento de las basadas en monitorizar actividad y reaccionar rápidamente ante posibles amenazas. Es algo que no sólo atañe a los servicios financieros, sino a toda la indústria con presencia online en general.

7. Siendo el financiero un sector altamente regulado, ¿cómo hace un CISO para balancear las necesidades de cumplimiento normativo con la gestión de riesgos de ciberseguriad?

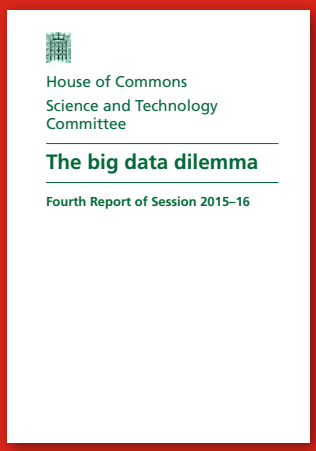
En nuestro caso combinando una separación de roles: el equipo de gobierno analiza todas las regulaciones que nos aplican y realiza los análisis gap necesarios, el equipo de protección lidera la implantación de los controles necesarios y el equipo de ciberseguridad adapta sus procesos de análisis y respuesta acorde con los mismos. Estar coordinados bajo una misma dirección y disponer de los medios necesarios, nos permite dar respuesta muy rápida a las nuevas, y cada vez más numerosas, exigencias en materia de cumplimiento. Y, por descontado, todo el proceso queda supervisado y auditado por otras áreas independientes dentro de la organización.

4 Informes y análisis sobre ciberseguridad publicados en febrero de 2016

Impact evaluation on the implementation of Article 13a incident reporting scheme within EU (ENISA)

Amenazas y analisis de riesgos en Sistemas de Control Industrial (ICS) (CCN-CERT)

The Big Data Dilemma (UK House of Commons)

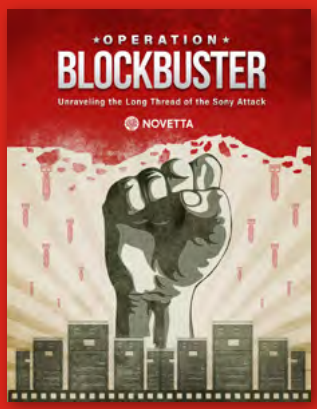


Communication network interdependencies in smart grids (ENISA)

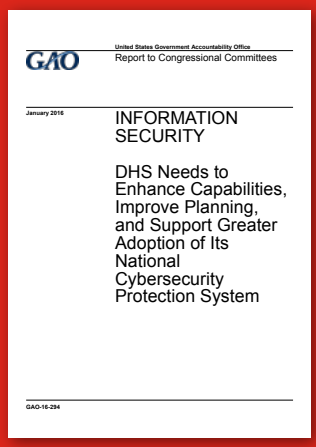
Emerging Cyber Threats and Implications (RAND)

Global Economic Crime Survey 2016 (PWC)

Operation Blockbuster (Novetta)



DHS Cybersecurity Protection System (GAO)



5 HERRAMIENTAS DEL ANALISTA: Cymon

Cymon es uno de los mayores trackers de información de seguridad de código abierto sobre phishing, malware, botnets y otras actividades maliciosas en internet. Entre otros permite la búsqueda de direcciones IP o de dominios en una amplia base de datos de reputación.

Cymon ingesta eventos y otras actividades maliciosas de casi 200 fuentes diariamente. En promedio, más de 15.000 direcciones IP únicas y 100.000 eventos son procesados cada día. La base de datos contiene más de 33 millones de evento de seguridad, de los cuales unos 6 millones corresponden a IPs únicas, y otros datos que provienen de fuentes y feeds comerciales y gubernamentales.

Ofrece una API totalmente funcional así como un motor de inteligencia abierto a la comunidad de investigadores y analistas, de forma que puedan ejecutar investigaciones de forma colaborativa para combatir el cibercrimen.

Adicionalmente permite la creación de reportes e informes de tendencias de utilidad para la ejecución de análisis forenses.

6 Análisis de los Ciberataques del mes de febrero de 2016

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

CIBERCRIMEN

A mediados de mes diversos investigadores se hacían eco de una nueva cepa de ransomware, denominado *Locky.* Es un nuevo ransomware que ha sido liberado (muy probablemente) por el grupo *Dridex.* Así pues, no es de extrañar que esté bien preparado, como demuestra que el grupo encargado del desarrollo haya realizado una inversión importante en recursos, reflejándose en el nivel de madurez de la infraestructura subyacente.

Por otra parte, el 21 de febrero, *Clemente Lefebvre de Linux* Mint confirmó que unos atacantes desconocidos habían elaborado una versión modificada de la imagen ISO de Linux Mint Cinnamon con una puerta trasera en ella y, posteriormente, se modificó la web de Linux Mint para que apuntase a la misma. Se desconoce el número de descargas que se realizaron durante el periodo que estuvo activo, pero como medida preventiva inmediata la web estuvo deshabilitada durante varias horas

Aprovechando el momento estacional, en las víspera de San Valentín, decenas de tiendas de venta de flores online se vieron afectados por un DDoS según han indicado analistas de Incapsula. En su *blog* describen cómo 34 de sus clientes sufrieron un aumento en el tráfico de red entre el 6 y el 12 de febrero en los frontales web alcanzándose picos de tráfico muy elevado.

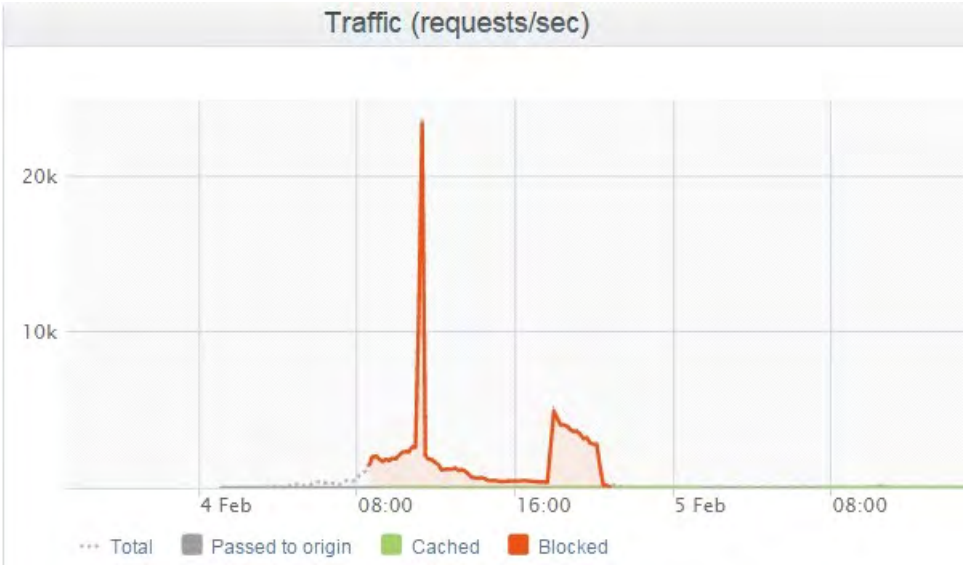
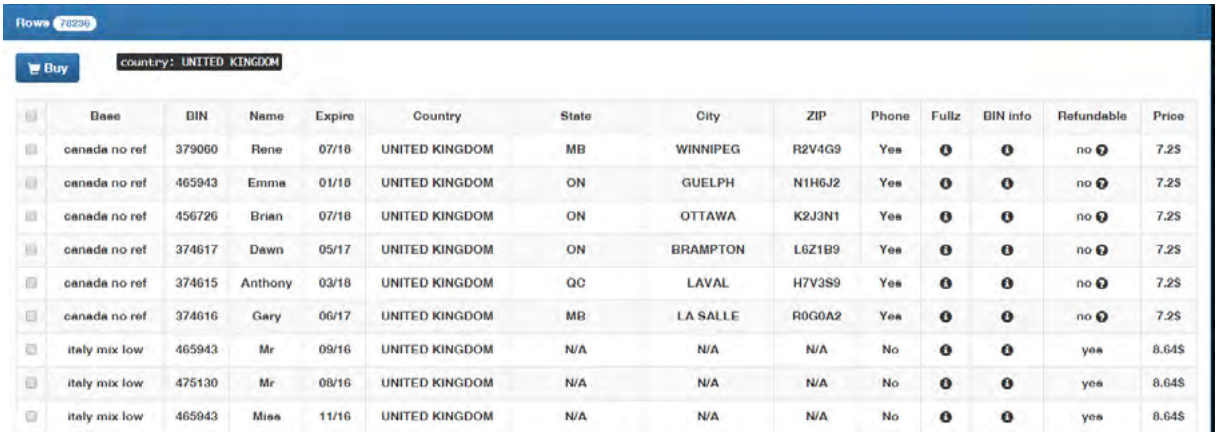


Ilustración Pico de tráfico de red asociado al DDoS sobre diversas tiendas de venta de flores online

A mediados de febrero, diversos medios de comunicación se hacían eco de la existencia de un grupo de cibercriminales que han sido detectados *vendiendo datos de tarjeta de crédito y débito robados a más de 100.000 ciudadanos británicos en un Marketplace llamado Bestvalid.cc*, siendo uno de los más grandes de este tipo.

En este portal web, por tan sólo 1.67 euros se pueden adquirir datos bancarios robados a más de un millón de personas en el mundo sin necesidad de acceder a la Deep Web.

La página web contiene información privada robada de un ex alto asesor de la Reina, así como de abogados, banqueros, médicos y otros profesionales.



Base	BIN	Name	Expire	Country	State	City	ZIP	Phone	Fullz	BIN info	Refundable	Price
canada no ref	379060	Rene	07/18	UNITED KINGDOM	MB	WINNIPEG	R2V4G9	Yes			no	7.2$
canada no ref	465943	Emma	01/18	UNITED KINGDOM	ON	GUELPH	N1H6J2	Yes			no	7.2$
canada no ref	456726	Brian	07/18	UNITED KINGDOM	ON	OTTAWA	K2J3N1	Yes			no	7.2$
canada no ref	374617	Dawn	05/17	UNITED KINGDOM	ON	BRAMPTON	L6Z1B9	Yes			no	7.2$
canada no ref	374615	Anthony	03/18	UNITED KINGDOM	QC	LAVAL	H7V3S9	Yes			no	7.2$
canada no ref	374616	Gary	06/17	UNITED KINGDOM	MB	LA SALLE	R0G0A2	Yes			no	7.2$
italy mix low	465943	Mr	09/16	UNITED KINGDOM	N/A	N/A	N/A	No			yes	8.64$
italy mix low	475130	Mr	08/16	UNITED KINGDOM	N/A	N/A	N/A	No			yes	8.64$
italy mix low	465943	Miss	11/16	UNITED KINGDOM	N/A	N/A	N/A	No			yes	8.64$

Ilustración Venta de tarjetas de crédito sustraidas en Bestvalid.cc

CIBERESPIONAJE

A comienzos de febrero, un *asaltante desconocido anónimo comunicó* que tenía en su poder los nombres, cargos, direcciones de correo electrónico y números de teléfono de más de 20.000 supuestos empleados de la Oficina Federal de Investigaciones (FBI), así como más de 9.000 de empleados del Departamento de Seguridad Nacional (DHS).

El hacker afirma también haber descargado cientos de gigabytes de datos de un ordenador del Departamento de Justicia (DOJ), a pesar de que los datos no han sido publicados todavía.

La Unidad 42 de Palo Alto Networks *publicó a comienzos de mes una investigación asociada a una campaña de cuatro años* cuya misión principal ha sido la recopilación de información acerca de los grupos de activistas minoritarios en China.

Palo Alto ha estado siguiendo al grupo tras la operación, al que han denominado Scarlet Mimic, durante los últimos siete meses. Sus objetivos eran principalmente los activistas de derechos sociales que representan a las minorías tibetana y uigur en China, así como a diversas agencias gubernamentales en Rusia y la India.

Los ataques más recientes tuvieron lugar en 2015 y, de acuerdo con los analistas de Palo Alto, muestran que Scarlet Mimic está interesado en obtener más información acerca de los activistas musulmanes y personas críticas contra el gobierno ruso.

El informe afirma que no hay evidencia alguna que vincule Scarlet Mimic a un actor gubernamental, por lo que "probablemente se trate de un adversario cibernético bien financiado y que gestiona hábilmente sus recursos", y que los motivos del grupo son similares a las posturas políticas expuestas por el gobierno chino.

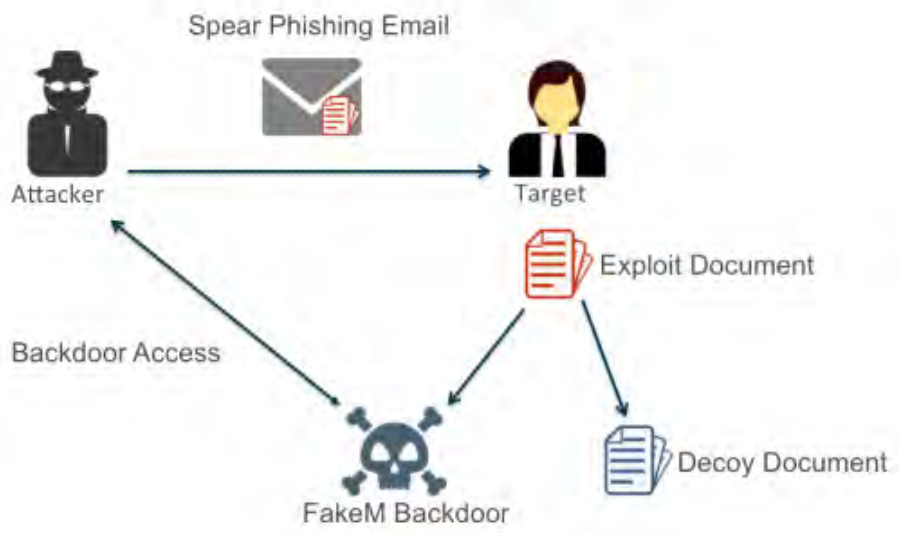


Ilustración Esquema de funcionamiento del vector de infección empleado por Scarlet Mimic

También a principios de febrero, se volvía a detectar el uso del software de vigilancia FinFisher, empleado para intervenir teléfonos móviles y ordenadores, en esta ocasión e*n un centro de datos de Sydney.* Así pues, se detectó su presencia en un servidor proxy dentro del centro de datos Global Switch en Ultimo, siendo utilizado para ocultar el usuario real del software espía, en este caso una agencia del gobierno de Indonesia, según un grupo de investigadores.

HACKTIVISMO

En el plano del hacktivismo, a mitad de mes se detectó un ciberataque sobre el hospital Hurley Medical Center norteamericano cuya autoría fue reclamada por Anonymous al parecer como una protesta por la crisis del agua de la ciudad de Flint.

A pesar de que el propio hospital negó cualquier tipo de impacto asociado al ciberincidente, diversas fuentes anunciaron que se produjeron problemas en los sistemas informáticos que generan etiquetas identificadoras para los pacientes así como en el sistema que gestiona qué tipo de menos deben ser suministrados a los diferentes pacientes.

Para finalizar, con ubicación en Chile, la Corporación Nacional de Desarrollo Indígena (CONADI) es una institución oficial, que formaparte del gobierno de Chile, dependiente del Ministerio de Desarrollo Social focalizada en prestar ayuda estatal, facilitar el acceso a la educación, prestar subsidios para la compra de tierras a la población indígena local.

Para acceder a estos beneficios, todos los indígenas deben registrarse recibiendo un certificado que prueba que son parte de la población indígena.

A finales de mes un grupo de hacktivistas chilenos denominados *Chilean Hackers (@ChileanCrew)* atacaron la web de CONADI, robando la base de datos publicando un enlace online a todos los datos completos en uno de los subdominios del dominio CONADI.CL, junto con un mensaje para la presidenta Michelle Bachelet, instándola a renunciar al cargo.

Curiosamente, uno de los reclamos del grupo hacktivista es forzar al gobierno chileno a poner más esfuerzo en la protección de los datos personales de la población indígena local.

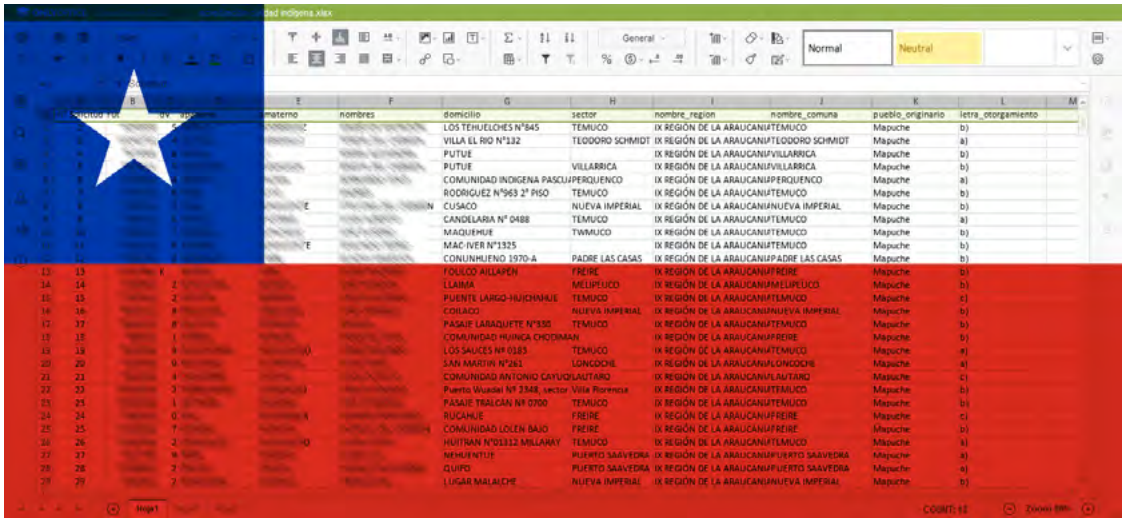
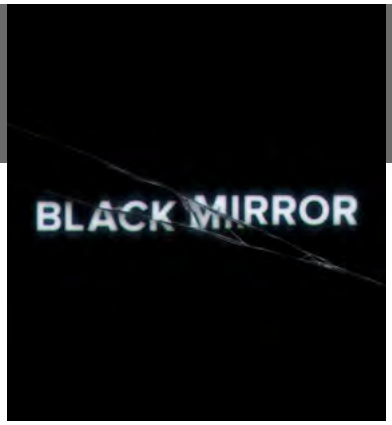


Ilustración Muestra del volcado de datos extraídos

Ilustración Defacemente de la página de Conadi

7 Recomendaciones

7.1 Libros y películas

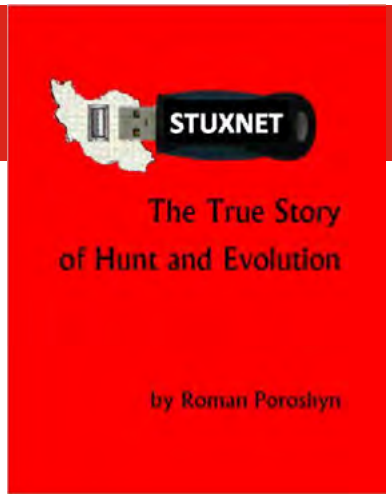


Serie:
BLACK MIRROR

Sinopsis: Black Mirror es una serie de televisión británica creada por Charlie Brooker y producida por Zeppotron. La serie gira entorno a cómo la tecnología afecta nuestras vidas, en ocasiones sacando lo peor de nosotros.

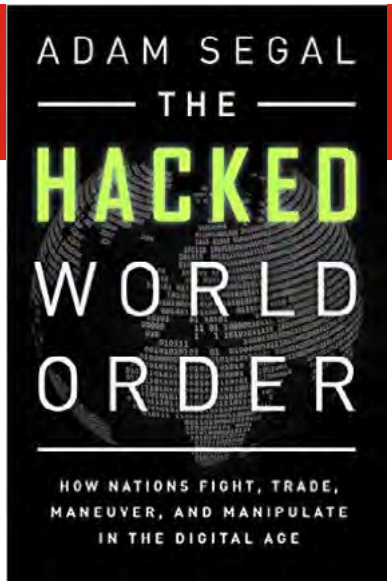
Película:
1984

Sinopsis: El futuro, año 1984. Winston Smith soporta una abyecta existencia bajo la continua vigilancia de las autoridades de la Oceanía totalitaria. Pero su vida se convertirá en una pesadilla cuando pruebe el amor prohibido y cometa el crimen de pensar libremente. Enviado al siniestro "Ministerio del Amor", se encuentra a merced de O'Brien, un cruel oficial decidido a destruir su libertad de pensamiento y a quebrantar su voluntad.



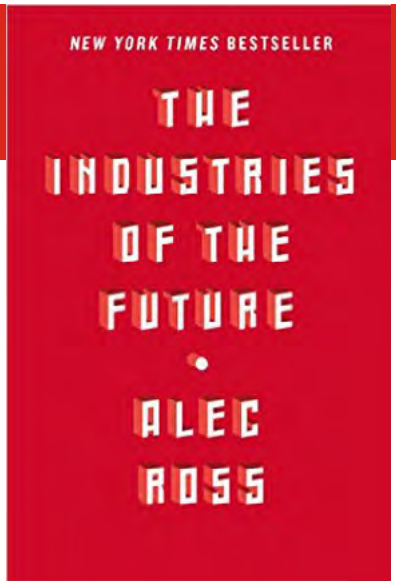
Libro:
STUXNET: THE TRUE STORY OF HUNT AND EVOLUTION

Autor: Roman Poroshyn
Num. Paginas: 172
Editorial: Amazon Digital Services LLC
Año: 2016
Precio: 8.00 Euros
Sinopsis: La historia del gusano Stuxnet está llena de sorpresas y giros inesperados que, sin duda, cambiaran su opinión sobre el presente y futuro de Internet y la World Wide Web.



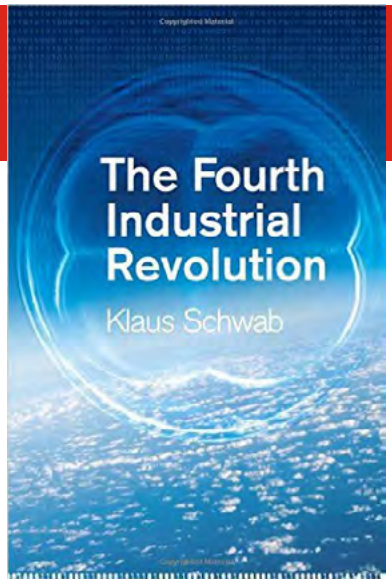
Libro:
THE HACKED WORLD ORDER

Autor: Adam Segal
Num. Paginas: 320
Editorial: Public Affairs
Año: 2016
Precio: 20.00 Euros
Sinopsis: A lo largo de la historia las naciones han ejercido la fuerza militar, la presión financiera, y la persuasión diplomática para crear el "orden mundial". Sin embrago, los ciberconflictos están redefiniendo un nuevo orden mundial donde las empresas tecnológicas se han convertido en actores principales.



Libro:
THE INDUSTRIES OF THE FUTURE

Autor: Alec Ross
Num. Paginas: 320
Editorial: Simon and Schuster
Año: 2015
Precio: 20.00 Euros
Sinopsis: El autor nos ilustra sobre los cambios que acontecerán en los próximos años, destacando las mejores oportunidades para el progreso y explicando las razones por las que algunos países prosperarán y otros no. Para ello, examina aquellos campos específicos que han de conformar nuestro futuro económico, tales como la robótica, la seguridad cibernética o la comercialización de la genómica, entre otros.



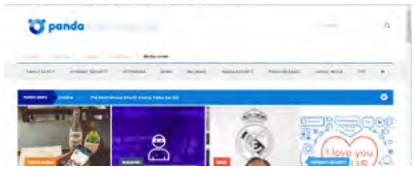
Libro:
THE FOURTH INDUSTRIAL REVOLUTION

Autor: Klaus Schwab
Num. Paginas: 198
Editorial: The Fourth Industrial Revolution
Año: 2016
Precio: 7.00 Euros
Sinopsis: El Profesor Klaus Schwab, fundador y presidente ejecutivo del World Economic Forum, reflexiona sobre el futuro que se está revelando hoy y cómo podemos asumir la responsabilidad colectiva para garantizar que es positivo para todos nosotros.

7.2 Webs recomendadas

http://www.hackplayers.com/
Blog nacional de referencia en materia de Hacking ético y seguridad informática.

http://www.pandasecurity.com/mediacenter/
Sitio web de la compañía PANDA que contiene toda la información que necesitas conocer sobre las amenazas en internet



https://staysafeonline.org/blog/
Blog del sitio web StaySafeOnline, dedicado a la concienciación en el uso responsable de las nuevas tecnologías.

http://blog.cybersecuritylaw.us/
Blog de la Universidad de Siracusa dedicado al análisis de los aspectos legales relacionados con la seguridad y defensa del ciberespacio.

https://niccs.us-cert.gov/
Sitio web del National Initiative for Cybersecurity Careers and Studies (NICCS) de los Estados Unidos.

https://www.acsc.gov.au/
Sitio web del Centro de ciberseguridad del gobierno de Australia

7.3 Cuentas de Twitter

@hackplayers

@mercemolist

@twittersecurity

@sch3m4

@BorjaMerino

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
29 febrero - 4 marzo	San Francisco	RSA	RSA Conference 2016	http://www.rsaconference.com/events/us16
1 Marzo	Londres	University of Salford	The Future of Cyber Security Conference	http://www.salford.ac.uk/onecpd/courses/the-future-of-cyber-security-conference-london
3-5 marzo	Madrid	Rooted	RootedCON 2016	http://www.rootedcon.es/
8 marzo	Ljubljana, Eslovenia	CSA	Cloud Security Alliance (CSA) CEE Summit 2016	https://csa-cee-summit.eu/
11-12 Marzo	Goa, India	Nullcon	Nullcon Security Conference	http://nullcon.net/website/
14-18 marzo	Heidelberg, Alemania	ERNW	TROOPERS16	https://www.troopers.de/
15-16 marzo	Blackpool, UK	North West Cyber Security Cluster	UK Cyber Security Conference 2016	http://www.cybersecurityconference.org.uk/
8 marzo / 10 marzo	Barcelona / Madrid	CODASIC	Tecnologías y servicios CASB (Cloud Access Security Broker).Extendiendo los controles corporativos de seguridad a la nueve pública	www.revistasic.com/respuestassic
29 marzo-1 abril	Marina Bay Sands, Singapur	Black Hat	Black Hat Asia 2016	https://www.blackhat.com/asia-16/
31 marzo-1 abril	Madrid	EuroCloud España	EuroCloud Spain	http://www.eurocloudspain.org/

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

https://www.linkedin.com/groups/7404269