REAL INSTITUTO elcano ROYAL INSTITUTE

DICIEMBRE 2016
Nº 20

CIBERelcano

Informe mensual de ciberseguridad

Desarrollado por: THIBER

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 Guillem Colom 11

4 Informes y análisis sobre ciberseguridad publicados en noviembre de 2016 .. 18

5 Herramientas del analista 19

6 Análisis de los ciberataques del mes de noviembre de 2016 22

7 Recomendaciones

7.1 Libros y películas 29

7.2 Webs recomendadas 32

7.3 Cuentas de Twitter 32

8 Eventos 33

1 COMENTARIO CIBERELCANO:
El Cyber Range, una capacidad estratégica

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

Fuente: thiia.org

Buena parte de los ciudadanos, la mayoría de las empresas y casi la totalidad de los gobiernos del globo son víctimas, a diario, de millones de **ciberataques** con un grado variable de sofisticación e impacto y, lo que es más preocupante, en su mayoría imperceptibles. La sustracción de información sensible o de datos de carácter personal, los ciberdelitos de naturaleza económica y el menoscabo e inutilización de sistemas militares, industriales, empresariales e incluso de infraestructuras críticas, son los principales objetivos de la gran mayoría de los ciberataques que acontecen hoy en día.

En este contexto, existe una creciente demanda de profesionales en el ámbito de la ciberseguridad por parte de gobiernos y empresas. La capacitación continua de estos profesionales es esencial para disponer de una ciberfuerza que permita establecer las medidas de seguridad apropiadas de los ciberespacios que protegen. Esta capacitación requiere de un nivel de innovación continuo únicamente proporcionado por entornos como los *Cyber Range*.

Un *Cyber Range* es una plataforma virtual que permite simular entornos operativos reales – estáticos o desplegables, clasificados o no clasificados - para la formación y el entrenamiento – individual o colectivo- de profesionales así como la experimentación, el testeo y la validación de nuevos conceptos, tecnologías, técnicas y tácticas de ciberseguridad y ciberdefensa.

Para que un *Cyber Range* sea eficaz deberá:

- Ser **accesible** en tiempo y forma por los profesionales autorizados para su utilización.

- Proporcionar un **entorno seguro** que permita a los usuarios ejecutar las actividades - formación, entrenamiento, experimentación, testeo y/o validación - sin poner en riesgo los sistemas en producción e información clasificada o sensible.

- Ser **escalable y flexible** para poder responder a las necesidades de los responsables en materia de ciberseguridad y ciberdefensa en función de la naturaleza de las actividades que lleven a cabo. No son equiparables los recursos necesarios para un curso de formación individual que para un ciber-ejercicio multinacional.

Esta fuera de cualquier duda que el Cyber Range es una capacidad estratégica que facilita y posibilita el cumplimiento de las estrategias de ciberseguridad y ciberdefensa de buena parte de gobiernos, organismos internacionales y empresas. En este sentido, la OTAN hace tiempo que identifico la necesidad de construir un Cyber Range como capacidad esencial para garantizar su defensa en el ciberespacio y la integración formal de la dimensión cibernética en el proceso de planeamiento de la defensa aliada.

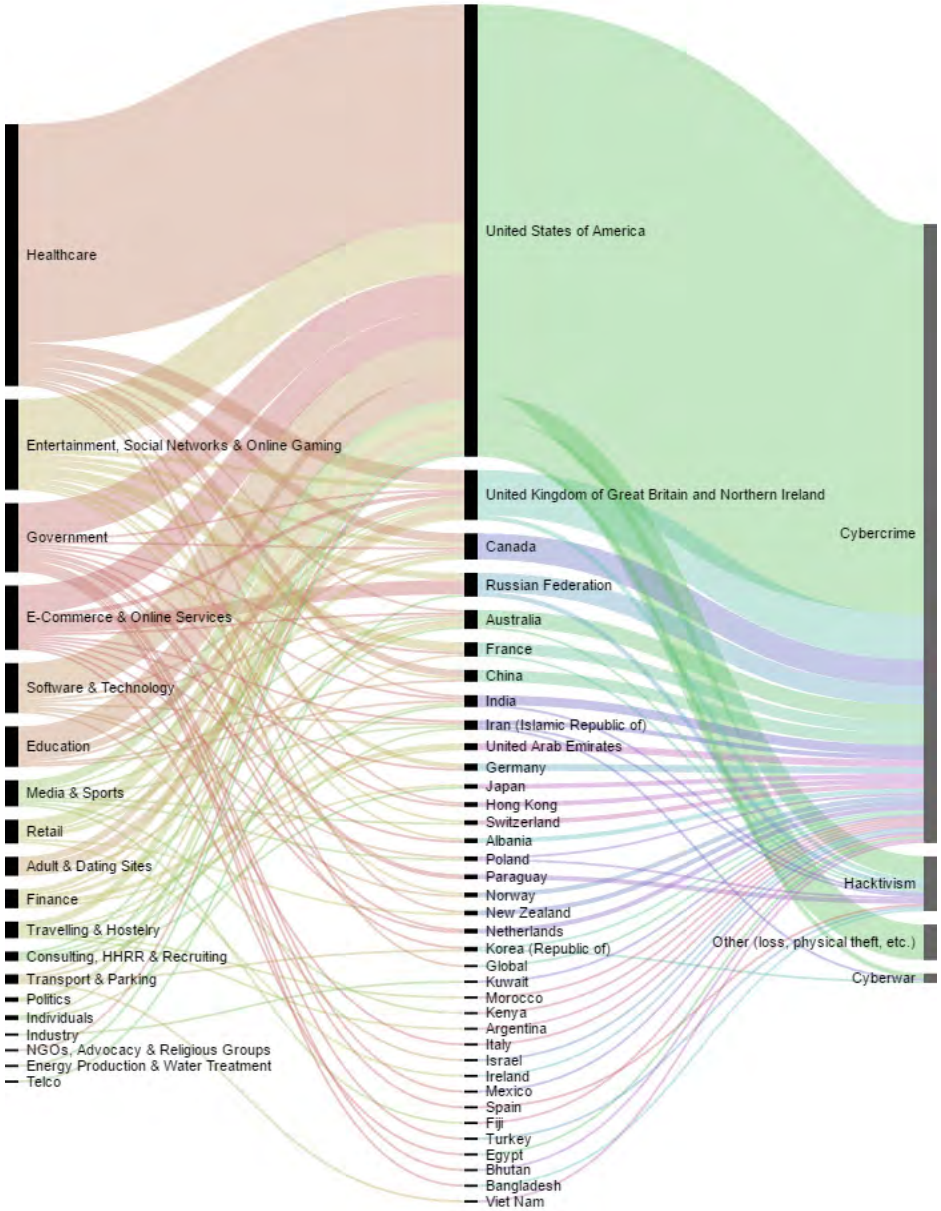
En definitiva, el **Cyber Range es una capacidad estratégica que posibilita que gobiernos y empresas puedan formar y entrenar de manera efectiva a sus profesionales así como experimentar, testear y validar nuevos conceptos, tecnologías, técnicas y tácticas de ciberseguridad y ciberdefensa.**

"La capacitación de los profesionales de ciberseguridad requiere de un nivel de innovación continuo únicamente proporcionado por entornos como los Cyber Range"

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
EEUU y el sector sanitario: los ciberataques se disparan.

AUTOR: Yaiza Rubio, Analista de THIBER, the cybersecurity Think Tank. Analista de inteligencia de ElevenPaths.

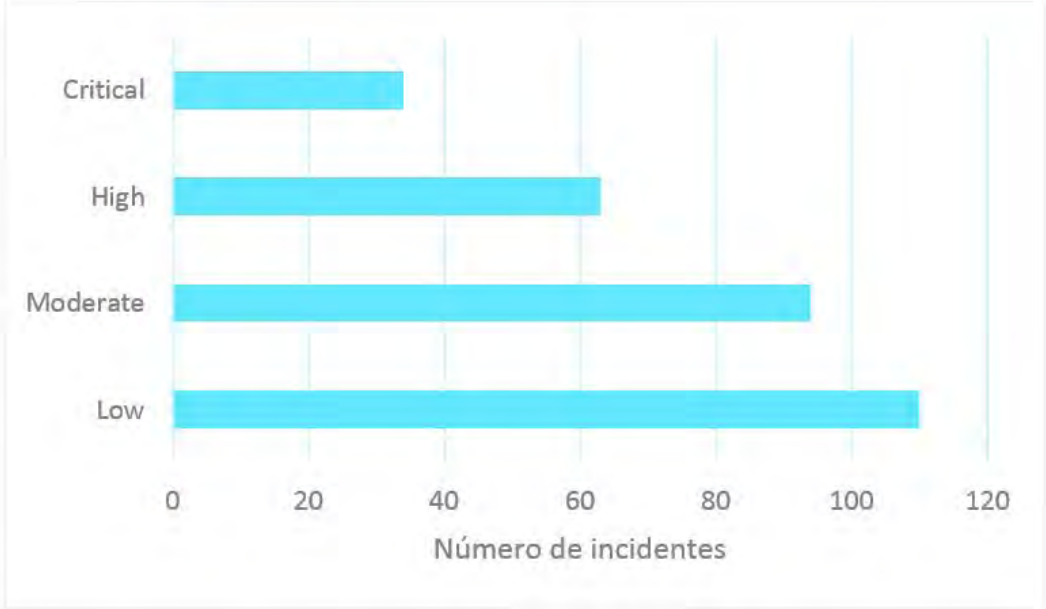
Son muchos los sectores que han sido objetivo de incidentes de ciberseguridad a lo largo del segundo cuatrimestre de 2016 pero, sin duda, una parte importante ha estado vinculada al sector sanitario de Estados Unidos, tal y como señalan algunas firmas de seguridad. El informe llamado *Las grandes fugas de información del segundo cuatrimestre de 2016* también resalta como plataformas más afectadas las asociadas al entretenimiento, las redes sociales y las gubernamentales respondiendo a intereses principalmente cibercriminales.



Incidentes del segundo cuatrimestre de 2016 por sector, país y motivación. Fuente: ElevenPaths.

Este cuatrimestre ha sido prolífico en cuanto a lo que se refiere a la filtración de información personal. Las 302 filtraciones identificadas en este período han dado lugar a más de 1.345 millones de registros expuestos en la red, lo que supone un incremento significativo respecto al *cuatrimestre anterior* y, especialmente, con respecto a las tendencias observadas también en *2015.*

En cuanto a la criticidad de las fugas de in-formación identificadas, revela la publicación de 34 filtraciones de carácter crítico lo que supone más del 300% de las *identificadas en el primer período del año.* Entre las que más repercusión han adquirido en los medios de comunicación se encuentra la de *Myspace*, *Linkedin*, Badoo, *Neopets* o *iMesh* con riesgo máximo y también otras como *Dropbox*, Tumblr, Zoosk o *R2Ga-mes* con un nivel de riesgo ligeramente menor.



Si atendemos a cuáles han sido los autores más representativos, la referencia fundamental es *Peace o peace_of_mind* que ha consolidado en este plazo su posición como una de las cuen-tas de referencia en la divulgación de bases de datos de credenciales. Tras ofertar en mercados de compraventa algunas de las bases de datos de mayor impacto mediático, esta ciberidentidad se ha convertido en un icono que, aun siendo bases de datos antiguas y publicándolas poco tiempo después a través de canales privados, han permitido al usuario conseguir monetizar sus acciones.

Otros autores que han filtrado información son conocidos de otros análisis publicados con anterioridad. Perfiles como SonnySpooks, 0x2Taylor, Ghost Squad Hackers o bRpsd son también cuentas reconocidas en el ámbito de la filtración pública de fugas de información. En cualquier caso, la identificación de muchos de estos perfiles como difusores de fugas de información no necesariamente implica que se trate de los filtradores originales, dado que se podría tratar de cuentas que se hacen eco de estas filtraciones tras conseguirlas en foros especializados.

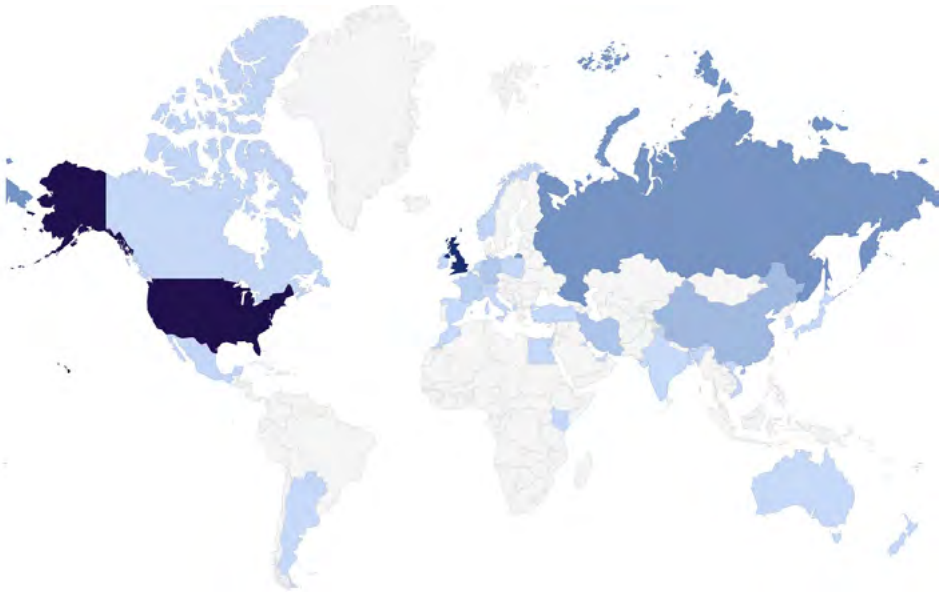
Volumen de credenciales filtradas

El número de sectores afectados se ha reducido. La publicación de una gran cantidad de bases de datos vinculadas a redes sociales y

plataformas de videojuegos (*MySpace*, *Twitter*, Tumblr son buenos ejemplos) ha acaparado gran parte de las credenciales expuestas, seguidos por otros que también aparecen de forma recurrente entre los más afectados: las plataformas de comercio electrónico, los sitios gubernamentales y las plataformas para adultos y vinculadas a sitios de citas.

Volumen de credenciales filtradas por sector. Fuente: ElevenPaths.

Atendiendo a la localización de los servicios afectados, prácticamente cuatro de cada cinco credenciales filtradas en este tiempo se corresponden con credenciales pertenecientes a plataformas situadas en Estados Unidos. Entre el resto de países afectados destacan también el Reino Unido (país en el que se ha enmarcado las fugas de Fling y de Badoo) y Rusia (especialmente señalada por la filtración de Mail.ru).



Volumen de credenciales filtradas por país. Fuente: ElevenPaths.

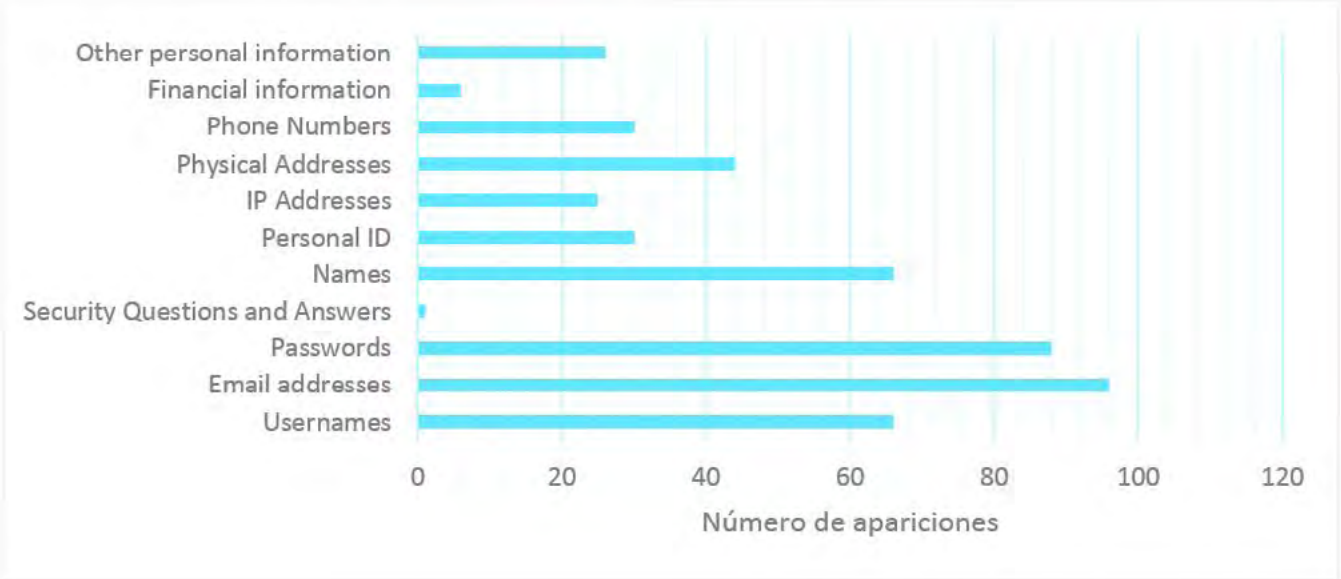
Naturaleza de la información filtrada

Como viene siendo habitual, uno de los aspectos que más lanza la proyección mediática de una fuga es la publicación de contraseñas junto con el resto de datos personales. Si se comparan los resultados con los *del primer cuatrimestre de 2016*, se ha observado que una parte significativa de las bases de datos filtradas ha expuesto contraseñas *hasheadas* en sus diferentes formatos.

Entre los motivos que están detrás de dicho cambio de tendencia, se encuentra el perfil alto de muchas de las plataformas que han sido víctimas de las grandes fugas de información publicadas durante estos cuatro meses. El hecho de que plataformas del calado de *Linkedin*, *Dropbox* o *Myspace* se hayan visto implicadas ha provocado, por un lado, fugas de información masivas que han afectado a millones de usuarios y, por otro, ha puesto sobre la mesa la existencia de unas medidas de seguridad mínimas.

"Siguen siendo numerosas las filtraciones en las que también se puede asociar los perfiles a direcciones postales, direcciones IP y números de teléfono, lo que da una idea de la concreción del perfilado que se podría llevar a cabo."

Como ya ocurriera en versiones anteriores de este informe, las filtraciones de este período han expuesto información de distinta naturaleza. Entre los campos más repetidos son correos electrónicos, *passwords* (tanto en texto plano como *hasheadas*) y alias y nombres completos. Siguen siendo numerosas las filtraciones en las que también se puede asociar los perfiles a direcciones postales, direcciones IP y números de teléfono lo que da una idea de la concreción del perfilado que se podría llevar a cabo. Especialmente significativa es también la información vinculada a datos de carácter personal de alta protección que incluirían información relativa a registros médicos, información policial y gustos y/o preferencias sexuales.



Qué hacer tras conocer que he sido afectado

La información robada y expuesta en la red de estos incidentes podría llegar a ser reutilizada. Desde el punto de vista de un atacante, contar con acceso a información personal es un elemento que puede ser explotado en diferentes formas de extorsión. De forma similar, la información también podría servir para configurar ataques dirigidos con mayores probabilidades de éxito utilizando los datos personales filtrados.

De cara a minimizar dicho riesgo, se debe evitar la reutilización de contraseñas en diferentes plataformas, además de cambiarlas periódicamente. De la misma manera, se aconseja la utilización de gestores de contraseñas que se encarguen de generar versiones complejas de estas donde el usuario solamente necesitará recordar una única password. Además, es preferible que en aquellas plataformas que así lo permitan se utilicen los sistemas de autenticación en dos pasos como medida de seguridad adicional que protegerá al usuario frente a intentos de conexión no autorizados.

"Desde el punto de vista de un atacante, contar con acceso a información personal es un elemento que puede ser explotado en diferentes formas de extorsión"

3 Entrevista a Guillem Colom.
Director de THIBER, the cybersecurity Think Tank

1. Has publicado recientemente la obra "De la compensación a la revolución: la configuración de la política de defensa estadounidense contemporánea (1977-2014)" donde argumentas que Estados Unidos ha logrado una Revolución en los Asuntos Militares (RMA). ¿Qué relación tiene que ver esta revolución con la importancia adquirida por lo ciber en el ámbito militar?

Tiene mucho que ver. Aunque es importante recordar que la tecnología es uno de los múltiples componentes de una "capacidad militar" (los otros pueden ser el personal, la doctrina, las infraestructuras, la organización o el adiestramiento), y que ésta por sí sola difícilmente transforma la forma de combatir, en esta última revolución que Estados Unidos ya ha conquistado y que ahora parece buscar una nueva RMA en el horizonte 2030, las tecnologías de la información han tenido un papel fundamental.

De hecho, han sido los avances tecnológicos que se han producido desde la década de 1970 en los campos de la informática, las telecomunicaciones o la robótica los que han transformado el arte de la guerra. Enfocadas originalmente a batir las fuerzas mecanizadas del Pacto de Varsovia en una hipotética guerra en Europa, estas tecnologías pronto se combinaron con nuevos conceptos operativos que permitieran explotar su potencial. Así, en la década de 1990 se consideró que lo realmente relevante revolucionario es que plataformas, sensores, armas y combatientes – inicialmente diseñados para operar

de forma aislada e incapaces de comunicarse entre ellos – pudieran interconectarse y trabajar en red. Y de la misma manera que nuestro ordenador puede comunicarse con otros ordenadores o sincronizarse con nuestro *smartphone* y *tablet* o trasvasar datos a la nube, este ecosistema militar permite a cualquier soldado conocer y controlar 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, precisamente, la premisa sobre la que se fundamenta el concepto *sistema de sistemas* que, calificado como la esencia de la RMA, permite 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. Esto sentaría a su vez el concepto de guerra u opera-

ciones en red que se ha convertido en la base sobre la cual operan las fuerzas armadas estadounidenses y desarrollan los conceptos futuros de empleo de la fuerza. Fundamentada en las posibilidades que brinda el *sistema de sistemas*, ésta permite que una fuerza conjunta, integrada en red y distribuida geográficamente por el campo de batalla opere con gran coordinación, flexibilidad, rapidez, precisión y seguridad.

2. Pero además de la integración de sistemas, hemos observado que lo ciber se ha convertido en la quinta dimensión del entorno operativo tras la tierra, los mares, los cielos y el espacio.

Exacto, Estados Unidos primero y muchos otros países después han pasado a considerar lo ciber como la quinta dimensión del campo de batalla. De hecho, podríamos afirmar que la pasada RMA ha creado dos nuevas dimensiones militares – el espacio y el ciberespacio – siendo la primera un facilitador y multiplicador de las operaciones porque el grueso de las capacidades de observación, reconocimiento, comunicaciones, geolocalización, mando y control, navegación, adquisición de objetivos o meteorología las proporcionan los satélites, y la segunda tanto un habilitador como una dimensión con entidad propia.

Recordemos, en este sentido, que en el ciberespacio transita el grueso de los flujos de información y comunicaciones necesarias para el planeamiento y conducción de las operaciones. De hecho, por el ciberespacio militar circulan tanto las coordenadas sobre las que situar en cualquier punto del globo sus unidades militares, la información procedente de sus medios de reconocimiento, las órdenes que deben ejecutarse, las coordenadas de los blancos a batir, los datos para dirigir sus drones y armas con precisión hacia sus objetivos o la información logística necesaria para sostener cualquier operación militar, por lo que para poder operar eficazmente, requieren de redes robustas, fiables, seguras y resilientes. En consecuencia, no parece raro que lo ciber sea tan importante, pues las operaciones en el ciberespacio pueden orientarse a

la protección, explotación, disrupción o destrucción de las redes, infraestructuras, equipos informáticos, sistemas tecnológicos o información almacenada con el objeto de disuadir al adversario de iniciar una acción militar, paralizar sus sistemas de defensa, desarticular sus fuerzas, erosionar sus capacidades de mando y control e incluso colapsar el país. En este sentido, a pesar de que en los últimos años hemos podido observar ciberataques preparatorios o complementarios a las operaciones militares tradicionales, es muy probable que en los próximos años veamos cada vez más ciberoperaciones de mayor complejidad e impacto.

"La Revolución en los Asuntos Militares consolidó el ciberespacio como entorno operativo"

3. Ello significa que las fuerzas armadas actuales son muy dependientes del ciberespacio para realizar sus labores habituales. ¿Qué problemas tiene esta dependencia?

En primer lugar, esta creciente exposición de las fuerzas armadas las puede hacer, si no toman las medidas correspondientes en materia de ciberdefensa, concienciación de su personal y obtención tanto de capacidades de respuesta y explotación como planteando formas de ciberdisuasión, muy vulnerables a los ciberataques, degradando su capacidad operativa y comprometiendo incluso la seguridad nacional. Pero existe otro elemento quizás menos evidente: la falta de ancho de banda. Las fuerzas armadas actuales son auténticas devoradoras de datos. Los flujos de información que deben soportar cada día las redes públicas y clasificadas de cualquier país de nuestro entorno se ha convertido en un problema de difícil solución – algo que se incrementa de forma exponencial cuando se trata de despegar fuerzas en operaciones – y una de las principales amenazas para la operatividad futura.

Por poner un ejemplo, actualmente se estima que las fuerzas armadas estadounidenses tienen una demanda de ancho de banda de 24 Gigabits por segundo, aunque muchos estudios independientes alertan que en los próximos cinco años esta necesidad se incrementará hasta alcanzar los 41 Gigabits por segundo, algo que las actuales redes no podrán soportar. Del mismo modo, solo el 22% de las comunicaciones estratégicas del país utilizan su propia red de satélites militares, mientras que el 78% restante emplean satélites comerciales con un coste anual de más de 2.000 millones de dólares. La última Revisión Cuatrienal de la Defensa de 2014 ya alertaba de esta situación y planteaba varias medidas encaminadas tanto a incrementar la capacidad de transmisión de datos de las infraestructuras cibernéticas del país, como para minimizar el impacto que podría tener la paralización de las redes en la operatividad de las fuerzas armadas.

En este sentido, la Armada estadounidense fue la primera en alertar de sus problemas de ancho de banda. Y no es extraño pensar que en un futuro no demasiado lejano éstos se incrementarán de forma exponencial a medida que los aviones de combate sean reemplazados por drones y los buques de superficie sean complementados por sistemas submarinos y de super-

ficie no-tripulados. La Fuerza Aérea y el Ejército de Tierra se hallan en una situación similar: la generalización del empleo de proyectiles de precisión e inteligentes y la progresiva introducción de robots en el campo de batalla requiere unos volúmenes de información que difícilmente las redes actuales podrán proporcionar y gestionar.

De hecho, esta es una de las preocupaciones que se halla detrás de la denominada Tercera Estrategia de Compensación que busca explotar las capacidades tecnológicas del país para incrementar la brecha militar entre Estados Unidos y sus adversarios, a la vez que garantizar la capacidad para proyectar su poder militar a cualquier punto del planeta con independencia de las defensas enemigas.

4. ¿Y qué pretende esta Tercera Estrategia de Compensación?

Aunque será cuestión de observar qué decisiones toma en materia de Defensa Donald Trump una vez sea investido Presidente de los Estados Unidos y cuáles son las prioridades en este ámbito que se deberán codificar en una nueva Revisión Cuatrienal de la Defensa, ya que algunas de las propuestas que ha realizado son difícilmente realizables o el coste económico que tendrían sería elevadísimo, es bastante probable que la Tercera Estrategia de Compensación guíe el planeamiento de la defensa del país en el horizonte 2030 y su consolidación motive una nueva RMA.

Fundamentada en la herencia de la RMA y enfocada a explotar el potencial científico-tecnológico del país, esta iniciativa pretende incrementar la brecha de capacidades militares entre Estados Unidos y sus potenciales adversarios, proyectar su poder a cualquier punto del globo con independencia de las estrategias Anti-Acceso y Negación de Área enemigas (A2/AD) y reforzar los compromisos de seguridad existentes entre el país y sus aliados. Más concretamente, se pretende que esta estrategia:

- Combine los *sistemas heredados* – aquellos medios terrestres, navales y aéreos que actualmente se hallan en el inventario militar estadounidense – con el desarrollo de nuevos medios materiales que permitan a las fuerzas armadas del país mantener su brecha cualitativa frente a cualquiera de sus adversarios.

. Limite la dependencia que tiene Estados Unidos de las instalaciones navales, aéreas y terrestres que, situadas en las regiones avanzadas, son vitales para preposicionar hombres y material, garantizar el eficaz sostenimiento de las fuerzas desplegadas y proyectar el poder militar.
· Reduzca la dependencia que tienen las fuerzas armadas del país de las capacidades (observación, reconocimiento, comunicaciones, geolocalización, mando y control, navegación, adquisición de objetivos o meteorología) que proporcionan sus satélites civiles y militares.

· Aproveche la presencia y capacidad de proyección de su Fuerza Aérea y Armada o la eficacia de sus sistemas dirigidos por control remoto o autónomos.

· Explote la capacidad estadounidense para realizar ataques estratégicos de precisión susceptibles de batir cualquier objetivo enemigo tanto dentro como fuera del área de operaciones.

· Modele la nueva carrera de armamentos que se producirá entre Estados Unidos y sus competidores mediante la explotación de aquellas áreas tecnológico-militares en las que el país mantiene el liderazgo (sistemas no-tripulados, inteligencia artificial, ciberespacio, guerra submarina, ataque estratégico o integración de sistemas) y donde sus adversarios todavía carecen del *know-how* necesario.

· Aproveche las alianzas, acuerdos o convenios existentes entre Washington y sus socios con el fin de mejorar su posicionamiento estratégico y compartir los costes y responsabilidades de la defensa regional.

En este sentido, en materia ciber será interesante observar no sólo como el país intenta garantizar el ancho de banda que requerirán estas fuerzas, sino también como explota las capacidades que ofrece el *big data* o la computación cuántica para apoyar el desarrollo de esta estrategia.

5. Cambiando de asunto, antes has hablado de que inicialmente se había planteado lo ciber como una parte de la guerra informativa. ¿Qué nos podrías comentar de esto?

Aunque podríamos decir que este elemento ya ha sido superado, sí es importante comentar que la guerra informativa se ha valido de Internet para incrementar su papel. De hecho, recordemos que ahora organizaciones como la OTAN o la UE conciben –diluyendo el concepto inicial para el que se utilizó – que la "guerra híbrida" que Rusia está llevando a cabo contra occidente se basa en la propaganda y la información falsa de muchos de sus portales de noticias y un ejército de trolls al servicio del Kremlin.

En este sentido, recordemos que el uso de la información y la propaganda ha sido una constante de todos los conflictos desde la antigüedad, en los conflictos recientes hemos observado como Internet – y muy especialmente las redes sociales virtuales – permite a cualquier actor, tanto estatal como no-estatal, realizar operaciones informativas con una facilidad y efectividad asombrosas. Tenemos numerosos ejemplos en Israel, Líbano, Palestina, Siria, Ucrania, Crimea o el Estado Islámico, donde el empleo de plataformas multicanal y redes sociales como Facebook, Twitter, Instagram, Flickr o Youtube permiten recopilar un vasto volumen de información sobre su enemigo susceptible de transformarse en inteligencia útil para las operaciones y tam-

bién influir en la opinión pública propia, adversaria y neutral mediante actividades de propaganda y contra-propaganda. Precisamente por ello, muchos ejércitos han integrado la dimensión cibernética en las labores de comunicación estratégica; realizan operaciones de información (INFOOPS) y operaciones psicológicas (PSYOPS) en el ciberespacio; llevan a cabo actividades de inteligencia de fuentes abiertas (OSINT) en Internet e incluso explotan la valiosa información que proporcionan las redes sociales virtuales (SOCMINT).

6. ¿Esto tiene algún tipo de peligro para las fuerzas armadas?

Sin duda, aunque muchas fuerzas armadas se han subido al carro de las redes sociales de forma más o menos efectiva y con una estrategia más o menos clara con el objetivo de mejorar su comunicación estratégica, el uso personal que sus integrantes hacen de las mismas puede suponer tanto una amenaza para la seguridad nacional y un riesgo para las operaciones militares como representar un problema de comunicación pública.

En este sentido, las Fuerzas de Defensa de Israel (FDI) son un buen ejemplo de ello. Aunque éstas constituyen el ejemplo paradigmático del uso y explotación de las redes sociales, también están sufriendo varios problemas de difícil solución. De hecho, según sus propias estimaciones, aproximadamente el 70% de sus oficiales y suboficiales y el 95% de su tropa disponen de perfil personal en Facebook. No obstante, su uso inadecuado provocó que en el año 2013 se prohibiera a los soldados pertenecientes a unidades de inteligencia y operaciones especiales compartir en las redes sociales virtuales fotografías que revelasen su condición de militar, máxime tras algunos episodios que pusieron en peligro la seguridad del país y la reputación de sus Fuerzas Armadas. El servicio de mensajería instantánea Whatsapp también ha sido una importante fuente de problemas para las FDI y no debe descartarse que esta aplicación o sus equivalentes Telegram o Line puedan plantear graves problemas de seguridad para sus usuarios militares.

Además, las redes sociales virtuales también pueden ser utilizadas por los soldados como medio de protesta. Por ejemplo, el pasado mayo

una campaña realizada a través de Facebook de apoyo a un soldado israelí arrestado tras ser grabado mientras apuntaba con su arma a dos adolescentes palestinos en Cisjordania consiguió más de 120.000 “Me gusta”.

Del mismo modo, durante la actual escalada militar en Ucrania, el inadecuado uso de las redes sociales por parte de soldados rusos ha comprometido la Seguridad de la Operación (OPSEC) y puesto en duda la versión oficial de Moscú sobre su no implicación en el conflicto. En este sentido, las fotografías compartidas por el soldado Alexander Sotkinen en su cuenta de Instagram lo geolocalizaban dentro de las fronteras ucranianas, más concretamente entre los pueblos de Krasna Talycha y Krasny Derkul, ambos controlados por las fuerzas rebeldes. Otros soldados, como Vladislav Laptev o Mikhail Chugunov publicaron en su perfil de VKontkte – una red social rusa similar a Facebook – fotografías de los convoyes militares rusos desplazándose a la frontera ucraniana o declaraciones de que “dispararon toda la noche contra Ucrania”, tal y como confirmó posteriormente la inteligencia estadounidense mediante fotografías de satélites.

No obstante, puede que el caso más conocido y controvertido de los riesgos – en este caso estratégicos y políticos – que entraña el empleo de las redes sociales para la seguridad de las operaciones militares es el caso de Igor Girkin, líder separatista de la autoproclamada República Popular de Donetsk, felicitándose en la red social Vkontkte de haber abatido un avión de transporte ucraniano Antonov AN-26 cerca de la ciudad de Torez...un avión que resultó ser el vuelo MH-17 de Malaysia Airlines y en el que murieron trescientos pasajeros. Punto y a parte merecería el análisis de inteligencia empleando fuentes abiertas como redes sociales virtuales, fotografías y herramientas de geolocalización para identificar y situar al lanzador autopropul-sado del misil superfície-aire SA-11 (que forma-ba parte del sistema antiaéreo BUK) que derribó este avión.

El empleo de las redes sociales en el ámbito militar no sólo se ha convertido en una importante herramienta de comunicación estratégica, sino también en una amenaza para la seguridad de las operaciones militares, un altavoz para las protestas de los soldados y un riesgo para la imagen y reputación de sus fuerzas armadas.

“Aunque muchas fuerzas armadas se han subido al carro de las redes sociales, el uso personal que sus integrantes hacen de las mismas puede suponer tanto un riesgo para las operaciones militares como un problema de comunicación pública”

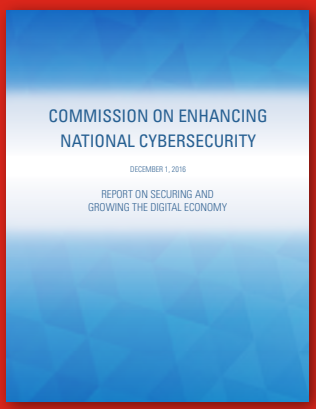
4 Informes y análisis sobre ciberseguridad publicados en noviembre de 2016

CISCO 2016 CyberSecurity Report (CISCO)

2017 Threats Predictions (McAfee Labs)

Strategic Principles for Securing the Internet of Things (U.S DHS)

Commision on Enhancing National Cybersecurity (The White House)



NCSS Good Practice Guide (ENISA)

Financial Cyber Threats Q3 2016 (Eleven Paths)

Cyber Insurance: Recent advances, Good Practices and Challenges (ENISA)

Estudio sobre Ciberseguridad y confianza en los hogares españoles (ONTSI)

5 HERRAMIENTAS DEL ANALISTA:
The Hive

A Scalable, Open Source and Free Incident Response Platform

TheHive es una solución escalable 3-en-1 de código abierto gratuita diseñada para facilitar la vida a los SOC, CSIRTs, CERTs y cualquier profesional de seguridad de la información que se ocupe de incidentes de seguridad que necesitan ser investigados y analizados con rapidez.

Como menciona el propio equipo de desarrollo de TheHive formado por profesionales experimentados en informática forense y respuesta a ciberincidentes, buscaron durante años una plataforma sólida y escalable para investigar y colaborar en incidentes de seguridad de la información, para almacenar objetos "observables" heterogéneos y para poder analizarlos uno a uno o en grandes cantidades.

Insatisfechos con lo que encontraron en el mercado, comenzaron a desarrollar TheHive en 2014.

Los principios base de la solución son:

Colaborar

La colaboración está en el corazón de TheHive. Múltiples analistas pueden trabajar en el mismo caso simultáneamente. Por ejemplo, un analista puede ejecutar un análisis de malware, mientras que otro puede trabajar en el seguimiento de la actividad de señalización de un servidor de comando y control (C2) en los logs proxy tan pronto como los IoCs (indicadores de compromiso) han sido agregados por su compañero de trabajo, gracias a Flow (un flujo de trabajo similar al timeline de Twitter que mantiene a todos actualizados sobre lo que está sucediendo en tiempo real).

Elaborar

Dentro de TheHive, cada investigación corresponde a un caso. Los casos pueden ser creados desde cero y las tareas agregadas sobre la marcha y enviadas a los analistas disponibles. También pueden crearse utilizando plantillas con

las métricas correspondientes para impulsar la actividad de un equipo, identificar el tipo de investigaciones que tardan mucho tiempo y tratar de automatizar tareas tediosas.

Cada tarea puede tener múltiples registros de trabajo donde los analistas contribuyentes pueden describir lo que están haciendo, cuál fue el resultado, adjuntar fragmentos de evidencia o archivos dignos de mención, etc.

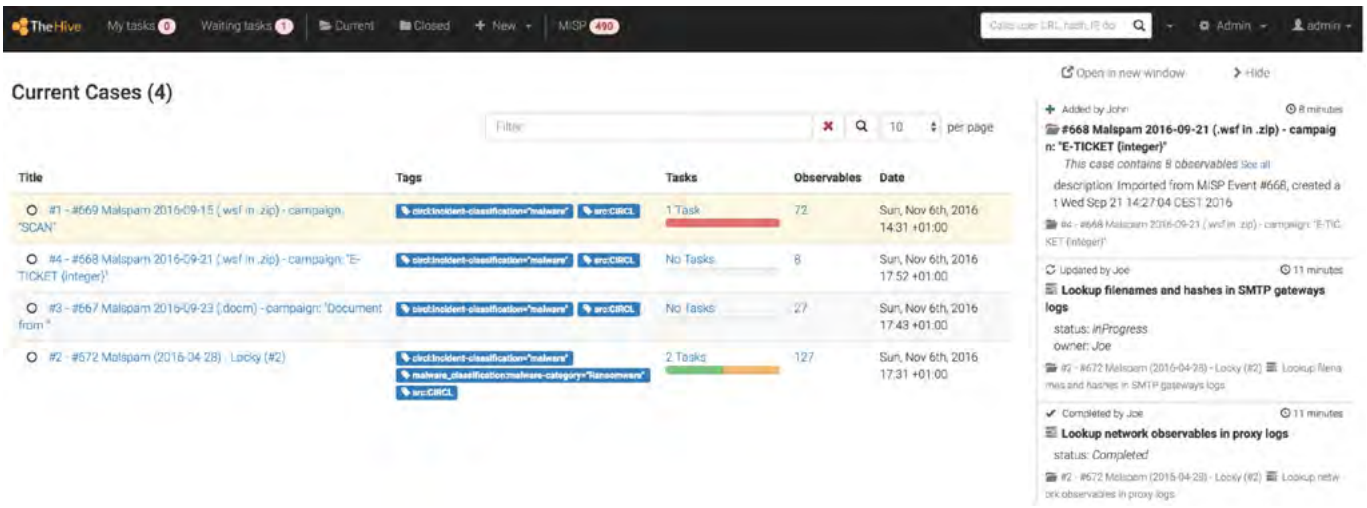
Analizar

Puede agregar uno o cientos si no miles de observables a cada caso que se cree. También puede crear un caso de un evento MISP ya que desde TheHive se enlace fácilmente a la instancia MISP desplegada. TheHive identificará automáticamente observables que ya se han visto en casos anteriores.

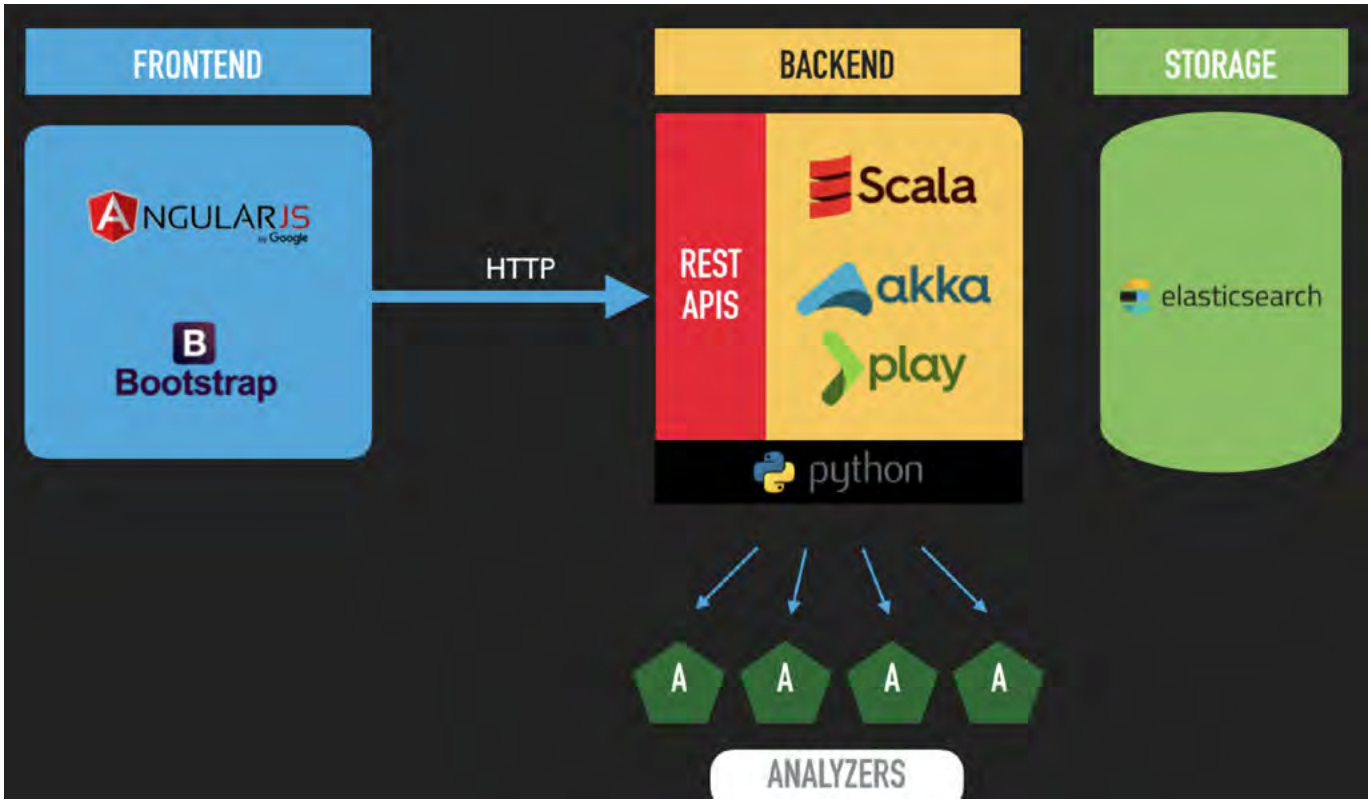
Observables también se pueden asociar con un TLP y su fuente (usando etiquetas). También puede marcar fácilmente observables como IOC y aislar a aquellos que utilizan una consulta de búsqueda y exportarlos para buscar en su SIEM u otros almacenes de datos.

TheHive también provee un motor de análisis. Los analizadores pueden escribirse en cualquier lenguaje de programación soportado por Linux como Python o Ruby para automatizar el análisis de objetos observables: geolocalización, búsquedas en VirusTotal, búsquedas de pDNS, análisis de mensajes de Outlook, búsquedas de amenazas, etc.

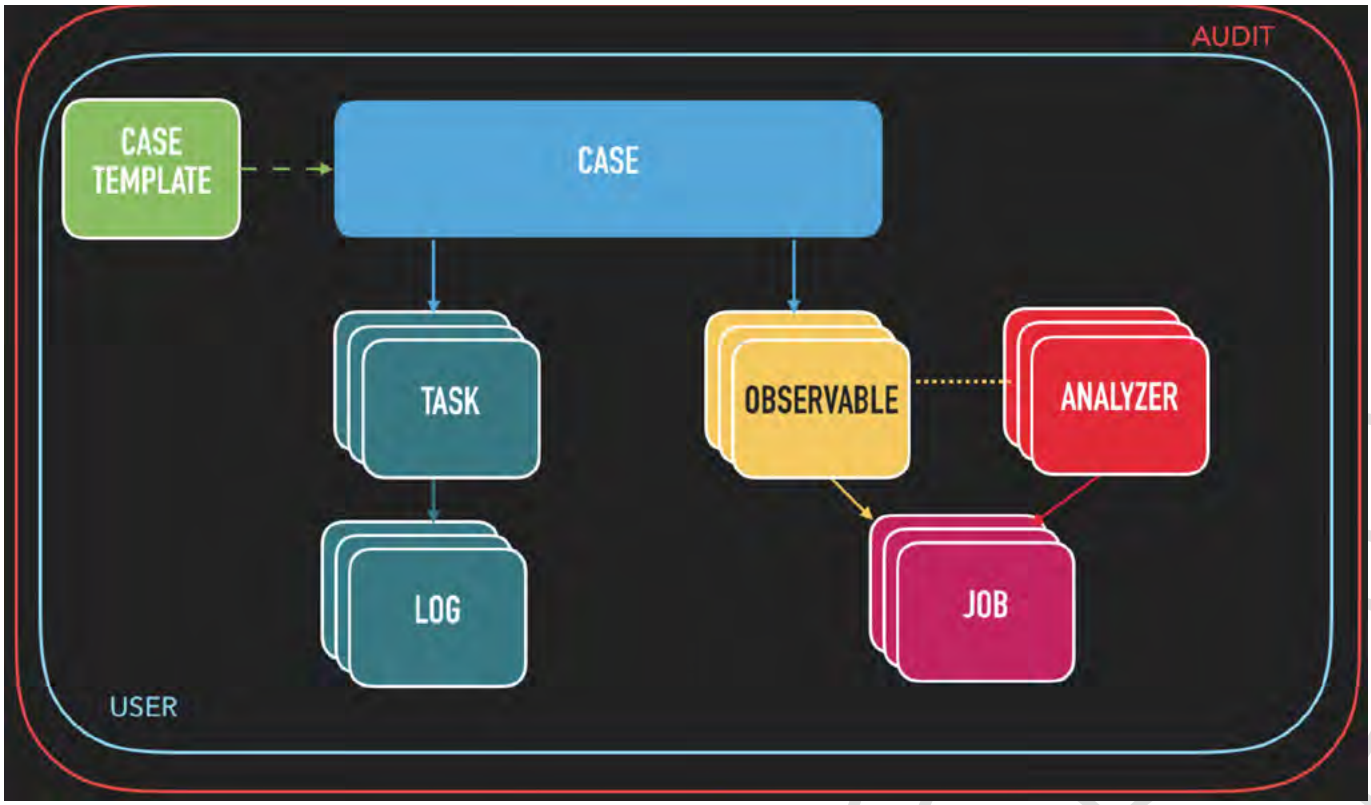
Los analistas de seguridad con habilidad para la creación de scripts pueden agregar fácilmente sus propios analizadores para automatizar las acciones tediosas que se deben realizar sobre observables o IoCs. También pueden decidir cómo se comportan los analizadores de acuerdo con el TLP.



Muestra de la consola web de administración



Arquitectura lógica de The Hive



Flujo de trabajo básico de la plataforma

6 Análisis de los Ciberataques del mes de noviembre de 2016

AUTOR: Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank.

CIBERCRIMEN

A comienzos del mes de noviembre, WikiLeaks, *la plataforma de denuncias dirigida por Julian Assange, había sufrido un ciberataque de denegación de servicio (DDoS) distribuido "dirigido"*, menos de 24 horas después de liberar más de 8.000 correos electrónicos nuevos del Comité Nacional Demócrata (DNC).

Esta publicación de información, lanzada menos de dos días antes de la fecha de las elecciones presidenciales de Estados Unidos, suponía el segundo gran leak de datos del Partido Demó-crata estadounidense tras la publicación de más de 50.000 mensajes personales del buzón de *entrada de John Podesta*, un colaborador cercano de Hillary Clinton.

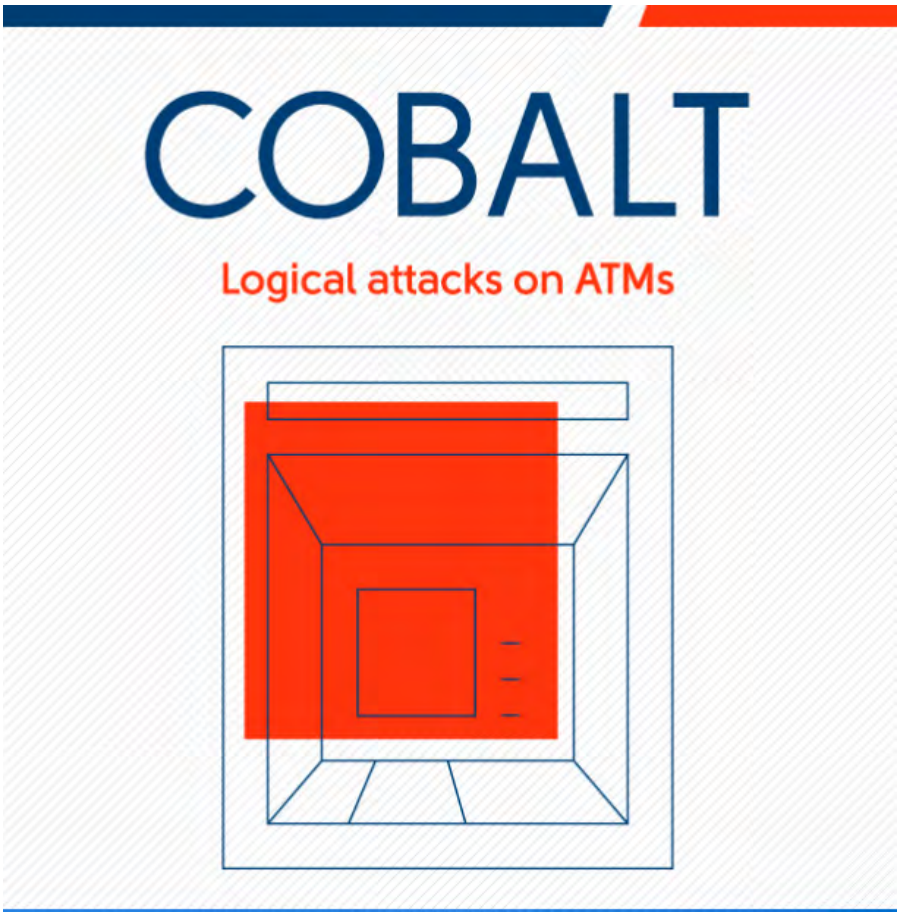
Conversación entre el director de comunicación del Partido Demócrata y Wikileaks

Según la firma rusa de seguridad cibernética Group IB, un grupo de ciberdelincuentes bajo una operación denominada COBALT, han atacado remotamente cajeros automáticos en más de una docena de países de Europa este año, utilizando software malicioso que forzaba a los cajeros a expedir dinero en efectivo.

Diebold Nixdorf y NCR Corp, los dos mayores fabricantes de cajeros automáticos del mundo, comunicaron que eran conscientes de los ataques y han estado trabajando con las entidades financieras para mitigar la amenaza. Los afectados más recientes en territorio europeo siguen la estela de los ataques a cajeros automáticos en Taiwán y Tailandia que fueron ampliamente reportados durante el verano.

Aunque los ciberdelincuentes han estado atacando cajeros automáticos con técnicas similares al menos durante los últimos cinco años, las primeras campañas involucraron en su mayoría un número pequeño de cajeros automáticos porque los hackers necesitaban tener acceso físico a las máquinas para hacerse con el efectivo.

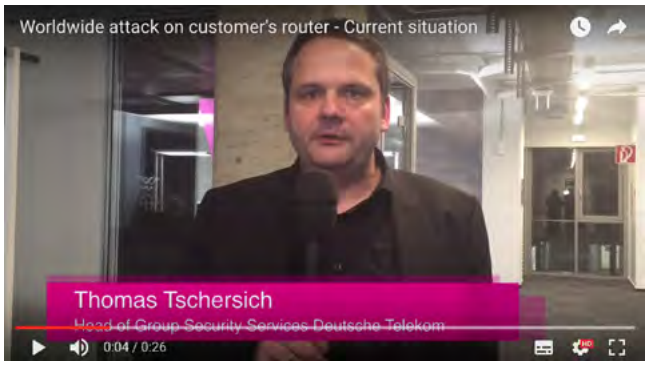
Sin embargo, las últimas campañas en Europa y Asia se llevaron a cabo desde mandos de centro y control, permitiendo a los criminales apuntar a un gran número de máquinas en operaciones con "muleros" que buscaban grandes cantidades de dinero antes de que los bancos descubriesen el ataque.



Por otra parte, el 23 de noviembre *se hizo público la notificación de la fuga de datos de carácter personal* e información sensible de más de 130.000 oficiales de la Marina de EEUU, tras un ataque de unos delincuentes sobre ordenador portátil de una subcontrata de la Marina, Hewlett Packard Enterprise.

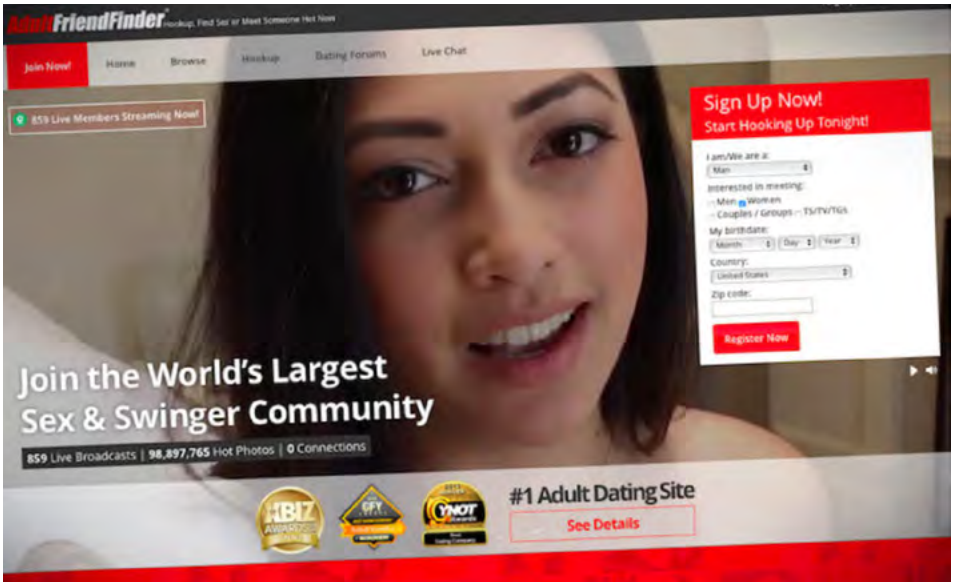
Web de la Armada de EEUU notificando el incidente

El 27 de noviembre, alrededor de 900.000 clientes de Deutsche Telekom en toda Alemania sufrieron un apagón en los servicios de internet, teléfono fijo, y acceso al servicio de televisión en línea, *según confirmó la compañía en un comunicado*, según el cual se indica que se está barajando un ataque cibernético como posible causa en el fallo del sistema. Según señaló André Hofmann, portavoz de Deutsche Telekom, el problema se ha registrado sólo en determinados tipos de routers, aparentemente afectados por un malware lanzado a través de la botnet Mirai explotando una vulnerabilidad de ejecución remota en SOAP.



Captura del video en el que Deustche Telekom informa sobre el ciberataque sufrido

En cuanto a los sitios de contenido adulto, de nuevo este mes ha sido muy difícil por los diversos ataques que han sufrido. Por una parte, *Leakbase revelaba* que se habían detectado intentos de comercializar una base de datos de 380.000 cuentas de usuario con información adicional sobre las preferencias y gustos de los afectados en algunos *markets* en la Deep web. Pero, sin duda, lo más notable ha sido el nuevo *leak* de información de la compañía de entretenimiento para adultos FriendFinder Network, que, tras un nuevo ciberataque, *ha sido víctima de una fuga masiva de datos exponiendo más de 412 millones de cuentas* y credenciales de usuario recolectadas durante dos décadas. Se cree que el ataque ocurrió en octubre empleándose direcciones de correo electrónico y contraseñas robados de seis sitios web para adultos de la FriendFinder Networks que habían sido previamente atacados (incluyendo cams.com y penthouse.com).



A finales de mes, diversos miembros del proyecto Tor *confirmaron la presencia de un exploit de día cero* ("0 day in the wild") que estaba siendo usado para ejecutar código malicioso en las equipos personales de usuarios de Tor y posiblemente otros usuarios del navegador Firefox.

En un trimestre tremendamente activo en cuanto a ataques de denegación de servicio distribuido (DDoS), *una de las últimas víctimas ha sido la Comisión Europea (CE)*. El día 29 fue objeto de un DDoS que conllevo una parada en los servicios de acceso a Internet durante varias horas. Si bien no se produjeron ataques colaterales simultáneos, el ataque provocó una pérdida de horas de trabajo significativas porque el personal no podía trabajar durante mucho tiempo. Los detalles de la identidad y la motivación de los atacantes no se han hecho públicos y la CE tampoco reveló las acciones tomadas para gestionar el incidente.

A principios de mes, *Tesco confirmó haber sufrido un "incidente sofisticado" contra su sistema transaccional.* El ataque contra el brazo bancario del gigante de supermercados británico implicó el robo de 2,5 millones de libras esterlinas de 9.000 cuentas de clientes, fondos que el banco reembolsó rápidamente. Inicialmente, el robo se temía que fuese contra 20.000 cuentas, pero esta cifra fue revisada a la baja unas horas más tarde.

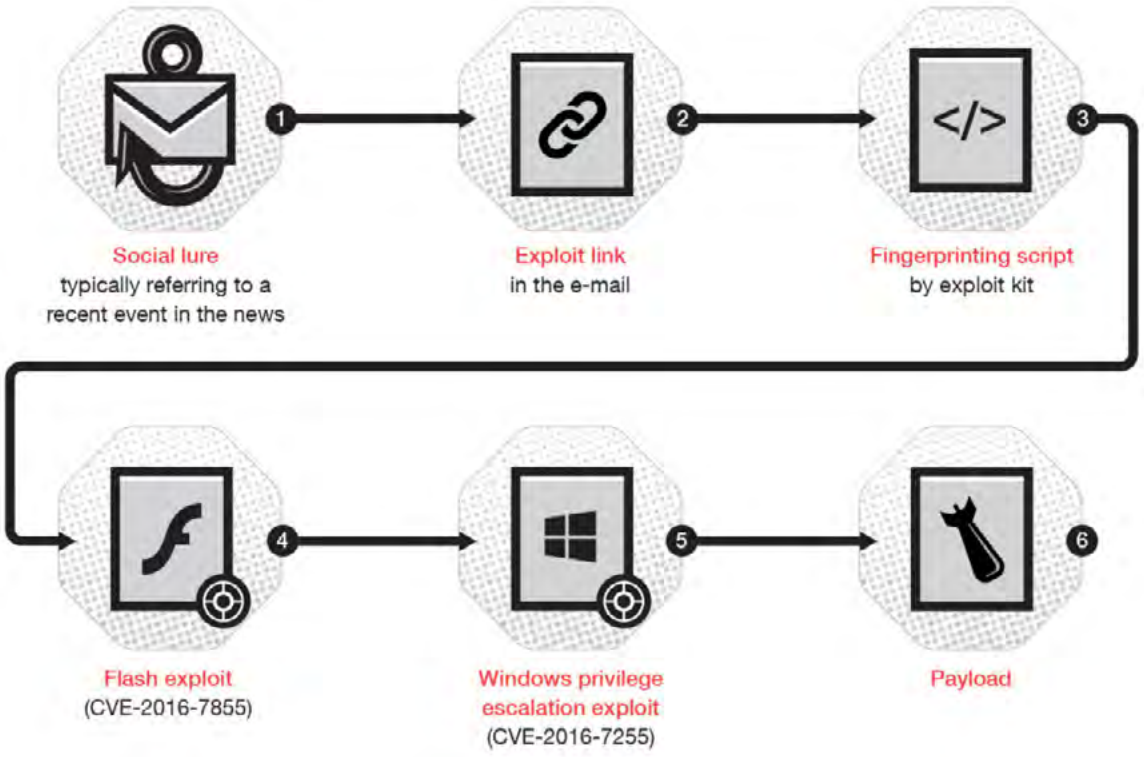
Tesco Bank gestiona alrededor de 136.000 cuentas corrientes. Diversos expertos en han culpado de forma provisional a un servicio de relleno de credenciales vulnerable, a la involucración de un trabajador interno y a los riesgos introducidos por una subcontrata de su cadena de suministro.

La NCSC británica está trabajando junto a la Agencia Nacional de la Delincuencia para estudiar el ciberataque, considerado es el más grande de su clase en la historia de la banca británica.

CIBERESPIONAJE

Fancy Bear, el grupo de ciberatacantes vinculado a Rusia, también conocidos como Pawn Storm, APT28, Sednit, Sofacy y Strontium, han maximizado la efectividad y vida útil de su vector de ataque a través de vulnerabilidades 0-day de Windows y campañas de spear-phishing, antes de que Microsoft y Adobe pudieran emitir los parches pertinentes.

El *equipo de analistas de seguridad de TrendMicro* descubrió que el mencionado grupo prolongó sus campañas en el tiempo explotando las vulnerabilidades 0-day contra diferentes actores gubernamentales y embajadas en todo el mundo, en los días previos al lanzamiento público de los parches por parte de los fabricantes.



Descripción del vector de ataque usado por Fancy Bears para distribuir el malware

También este mismo mes, pocas horas después de que Donald Trump fuera declarado victorioso en las elecciones estadounidenses, *el grupo de criminales, Cozy Bear (APT29), asociado por los medios occidentales al Kremlin, lanzó una ola de ataques contra blancos estadounidenses.*

El mencionado grupo, al que se le atribuye el controvertido ataque al Comité Nacional Demócrata (DNC) entre otros, ha sido identificado como el grupo responsable del ya conocido como "ciberataque post-electoral", dirigido a empleados que trabajaban en organizaciones como Radio Free Europe / Radio Liberty, la Corporación Rand, el Consejo Atlántico y los Departamentos de los Estados Unidos, según afirman fuentes cercanas a Washington y la firma de seguridad Volexity.

Tras las diversas manifestaciones acaecidas en el Reino Unido el pasado 5 de noviembre en conmemoración de la denominada Marcha Anual del Millón de Máscaras, *el colectivo Anonymous reclamó la autoría del ciberataque* que mantuvo caída durante más de ocho horas parte del portal web de Scotland Yard (concretamente el apartado *http://content.met.police.uk*) como represalia por las decenas de arrestos que se llevaron a cabo en la manifestación en el Parlamento de Londres.

Finalmente, a mediados de mes, el hacktivista conocido como *ElSurveillance ha actuado de nuevo bajo una operación denominada #EscortsOffline* y que han tenido como consecuencia la publicación de dos bloques de datos privados en internet pertenecientes a dos portales web independientes: 24luv.com (92.937 direcciones de correo electrónico de los usuarios y contraseñas en texto plano) y freedateusa.com (127.395 direcciones de correo electrónico y contraseñas en texto plano). Este hacktivista islamista advertía en un comunicado sobre las motivaciones de sus ataques.

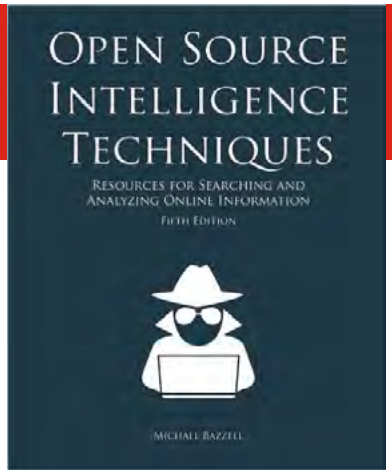
Mensaje dejado en la web 24luv.com

7 Recomendaciones

7.1 Libros y películas

Reportaje:
SHENZHEN: THE SILICON VALLEY OF HARDWARE

Sinopsis: Shenzhen es una de las primeras ciudades donde el gobierno chino experimento a finales del siglo XX con las propuestas de liberalización economica. Shenzhen,el Silicon Valley del Hardware es el primer capítulo de una nueva serie producida por Wired que aborda todo los aspectos relacionados con las ciudades del futuro y la tecnología.

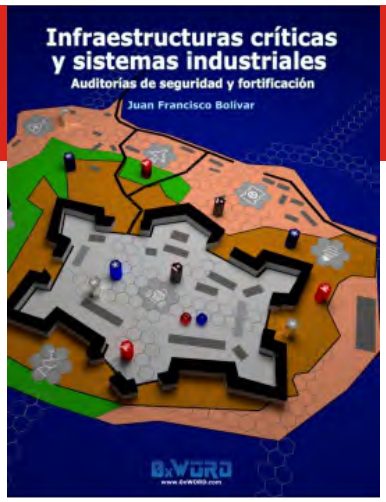


Libro:
OPEN SOURCE INTELLIGENCE TECHNIQUES

Autor: Michael Bazzell
Num. Paginas: 422
Editorial: CreateSpace Independent Publishing Platform
Año: 2016
Precio: 28.00 Euros
Sinopsis: A través de 16 capítulos, Michael Bazzell profundiza en las principales técnicas para la obtención de inteligencia en fuentes abiertas. Todas estas técnicas son presentadas en formato *hands-on* lo que facilitará y mejorará el aprendizaje del lector.

Libro:
CIBERSEGURIDAD, LA PROTECCIÓN DE LA INFORMACIÓN EN UN MUNDO DIGITAL

Autor: Fundación Telefónica
Num. Paginas: 145
Editorial: Ariel
Año: 2016
Precio: Gratuito
Sinopsis: Este monográfico ofrece una visión global de este problema y de cómo se puede abordar la seguridad en el mundo digital —ciberseguridad—, teniendo en cuenta el punto de vista de los usuarios tradicionales de Internet, el de las empresas usuarias y las que crean las tecnologías, y el de las Administraciones.



Libro:
INFRAESTRUCTURAS CRÍTICAS Y SISTEMAS INDUSTRIALES

Autor: Juan Francisco Bolivar
Num. Paginas: 224
Editorial: 0xWORD
Año: 2016
Precio: 22.00 Euros
Sinopsis: Entender que son las infraestructuras críticas, sus protocolos, componentes y configuraciones, es básico para enten-der cómo funcionan. Estas infraestructuras controlan los servicios básicos para todos los ciudadanos y sin los que su bienestar se vería comprometido. En este texto se explica el uso de dispositi-vos que actúan sobre el medio físico, pudiendo crear incidentes que trasciendan las barreras lógicas y actúen sobre el mundo físico, como los usados en Centrales Nucleares, conducciones de Gas, sistemas industriales... Aprender a detectar los puntos de ataque más débiles de estos sistemas, como realizar un pen-testing contra dispositivos como PLC's, HMI o SCADA será la principal misión de este libro. Ayudar a aquellos que se inician en los dispositivos industriales a realizar sus primeros ataques a estos sistemas, partiendo del conocimiento de ataques a las redes TI, aplicados a redes OT.

Libro:
HACKING WIRELESS NETWORKS

Autor: Andreas K. Kolokithas
Num. Paginas: 428
Editorial: CreateSpace Independent Publishing Platform
Año: 2015
Precio: 20.00 Euros
Sinopsis: El autor plantea 30 ejercicios prácticos a través de los cuales el lector podrá profundizar en las técnicas para una securización avanzada de la red Wi-Fi de su casa o negocio.

7.2 Webs recomendadas

http://www.astic.es/
Sitio web de la Asociación profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas.

https://www.govcert.admin.ch/
Sitio web del CERT gubernamental de Suiza

https://analysis.yararules.com/
Sitio web donde podremos encontrar reglas de YARA, aquellas que permiten la clasificación del malware.

http://www.pandasecurity.com/spain/
Sitio web de la compañía española Panda especializada en el desarrollo de soluciones de seguridad.

http://www.mundohacker.es/
Sitio web de Mundo Hacker , programa de televisión sobre ciberseguridad

https://www.certsi.es/
Sitio web del Centro de Respuesta a Incidentes Informáticos para Empresas, RedIRIS, Profesionales de TI e Infraestructuras críticas

7.3 Cuentas de Twitter

@SecMash

@cybersec4u

@Panda_Security

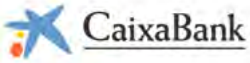
@_ASTIC

@GovCERT_CH

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
1- 4 diciembre	Leon	INCIBE	CYBERCAMP 2016	https://cybercamp.es/
5 - 8 diciembre	Estambul, Turquía	US Department of commerce	Cyber Security Trade Mission to Turkey	http://2016.export.gov/trademissions/cyberturkey/
5 - 7 diciembre	Barcelona	IEEE	The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016)	http://icitst.org/
12 diciembre	Nazareth, Israel	People & Computers	ICS CyberSec 2016 (Industrial Control Systems)	http://ics-cybersec-2016.events.co.il/
12- 14 diciembre	Londres	IEEE	World Congress on Industrial Control Systems Security (WCICSS-2016)	http://www.wcicss.org/
12 - 15 diciembre	Orlando, EEUU	ISC2	ISC2 Security Congress	http://congress.isc2.org/events/-isc-security-congress-2016/event-summary-993a0d888f31465eaf6cbcce7ac8c2e8.aspx
13 -14 diciembre	Madrid	CCN	X Jornadas STIC CCN-CERT	https://www.ccn-cert.cni.es/xjornadas
27 - 30 diciembre	Hamburgo, Alemania	Chaos Computer Club	Chaos Communication Congress 2016	https://events.ccc.de/2016/09/01/call-for-participation-33rd-chaos-communication-congress-en/

Patrocinadores



Consejo Asesor Empresarial

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269