REAL INSTITUTO elcano ROYAL INSTITUTE

FEBRERO 2017
Nº 22

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 Francisco Lázaro.....09

4 Informes y análisis sobre ciberseguridad publicados en enero de 2017 14

5 Herramientas del analista 15

6 Análisis de los ciberataques del mes de enero de 2017 17

7 Recomendaciones

7.1 Libros y películas 23

7.2 Webs recomendadas 26

7.3 Cuentas de Twitter.....26

8 Eventos.....27

1 COMENTARIO CIBERELCANO:
La ciberguerra de Trump (II)

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

Fuente: : New York Times

En los próximos días el Presidente Trump firmara su primera orden ejecutiva en materia de ciberseguridad. Dicha orden ejecutiva, *recientemente filtrada por el Washington Post*, no supondrá –salvo modificación de última hora- ninguna revolución respecto a las políticas y líneas de acción aprobadas en la materia por su antecesor Barack Obama, pero llevaran la firma del nuevo POTUS. Auditorias de las cibercapacidades de las principales agencias gubernamentales, análisis sobre el estado de madurez de las cibercapacidades defensivas y ofensivas del Departamento de Defensa y un plan para modernizar la infraestructura TIC del país son los 3 ejes principales sobre los que se articulará la citada orden. Igualmente, POTUS ha solicitado un análisis pormenorizado de las cibercapacidades de sus principales adversarios (y de sus principales aliados), aunque dicho análisis no debería demorarse ya que las agencia de inteligencia del país disponen de un "situational awareness" certero de las capacidades de terceros.

En el ámbito del Departamento de Defensa, James Mattis ha anunciado que tras las modificaciones propuestas al presupuesto del Departamento de Defensa la partida destinada a ciberdefensa alcanzaría los 60.000 millones de dólares, un 10% del total. Además, Mattis anuncio la prórroga del programa de *contratación de personal civil* del DoD que potenciara la contratación de personal especializado para el desarrollo, operación y mantenimiento de las capacidades cibernéticas del Pentágono. En este

sentido, resulta evidente que el Pentágono necesita un programa de captación y retención de talento que compita con la empresa civil y permita así la construcción de la ciberfuerza que necesita el Pentágono.

Además, desde hace unos meses el Pentágono estudia la posibilidad de que el U.S Cyber Command deje de ser un comando subordinado al U.S Strategic Command y adquiera la categoría de Mando Conjunto. Este hecho conllevaría que el U.S Cyber Command ejercería una dirección y control, en el sentido amplio, sobre las actividades en materia cibernética de los Ejércitos y la Armada. Del mismo modo, el Departamento de Defensa debate sobre la idoneidad de segregar el U.S Cyber Command y la Agencia de Seguridad Nacional (NSA), cuyas direcciones recae sobre el Almirante Michael S. Rogers, y sobre la ciberseguridad de las infraestructuras criticas del DoD se encuentran en el punto de mira de Trump.

En definitiva, el Presidente Trump es consciente de que a pesar de la inversión realizada durante las dos últimas décadas el nivel de ma-durez cibernético del país no es aún el deseado, lo que supone un riesgo para la seguridad y de-fensa del país.

"La primera orden ejecutiva de Trump en materia de ciberseguridad no suponen una revolución respecto a las políticas de Barack Obama"

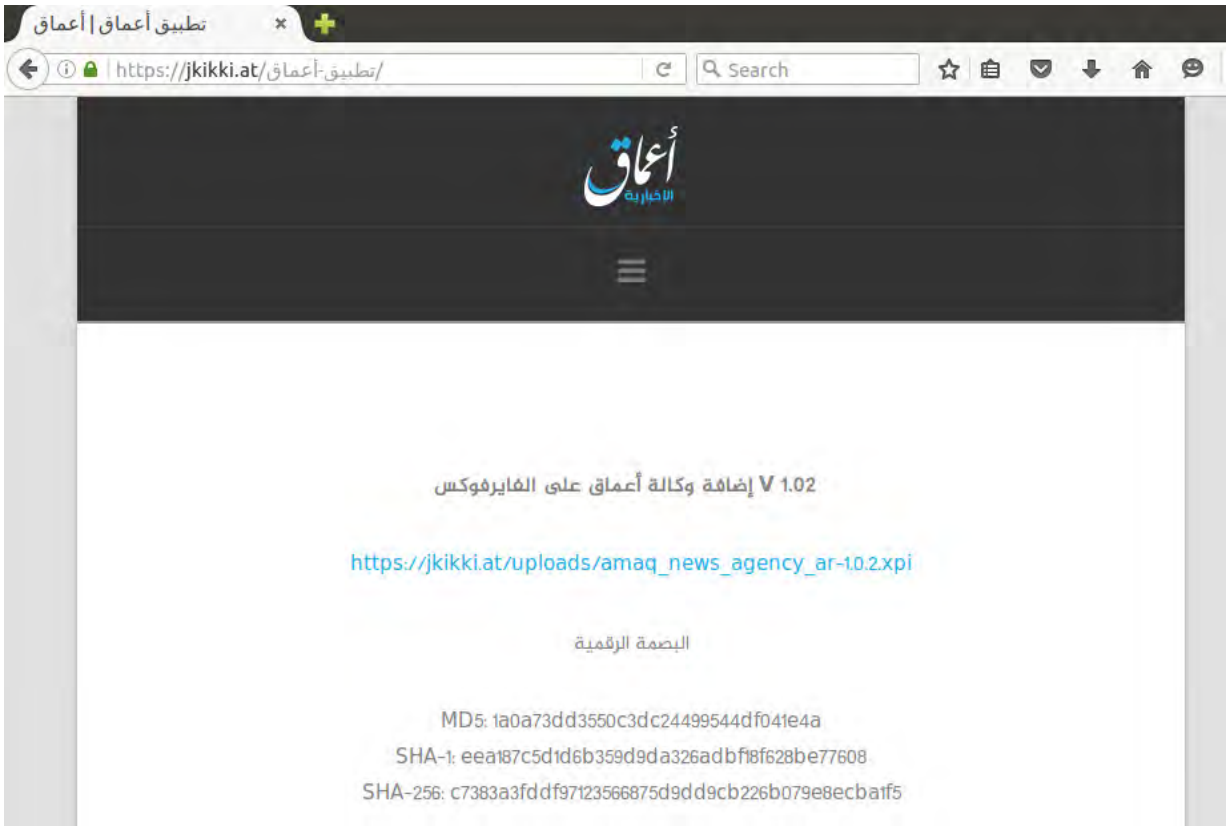
2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

Daesh y sus mecanismos de persistencia en internet

AUTOR: Yaiza Rubio y Félix Brezo, Analistas de THIBER, the cybersecurity Think Tank. Analistas de inteligencia de ElevenPaths.

2016 se cerraba con el anuncio público de la *alianza entre Facebook, Microsoft, Twitter y Youtube* para crear una base de datos compartida de imágenes y vídeos, y así comenzar a luchar de forma conjunta contra el ciberterrorismo en las redes sociales para frenar "la proliferación de contenido terrorista online". Sin embargo, parece que la estrategia de Estado Islámico está evolucionando hacia el concepto de hacer perdurable su propaganda en Internet al margen de las acciones conjuntas de las grandes compañías tecnológicas decididas ahora a combatir el terrorismo en su vertiente digital.

En este sentido, una investigación publicada a comienzos de enero por ElevenPaths a través de su *blog* , hacía eco del descubrimiento de complementos para navegadores web con el objetivo de facilitar a los usuarios, aún más, el acceso a sus contenidos. Aunque las extensiones de Firefox se distribuyen principalmente a través del mercado oficial de Mozilla, la Agencia de comunicaciones Amaq, identificada como medio propagandístico del Estado Islámico, estaría distribuyendo los ficheros con extensión .xpi, correspondiente a dichos plugins, a través de páginas web afines.



SOBRE LAS EXTENSIONES

Se han identificado dos versiones diferentes de la extensión, la 1.0.1 y la 1.0.2. Los ficheros se encuentran comprimidos en .zip y renombrados a .xpi. Estos son los que contienen el código Javascript, CSS y HTML y definen el comportamiento de la extensión. No obstante, los ficheros más interesantes son los siguientes:

- package.json contiene metadatos e información sobre la extensión como el nombre, autor, licencia y permisos requeridos.

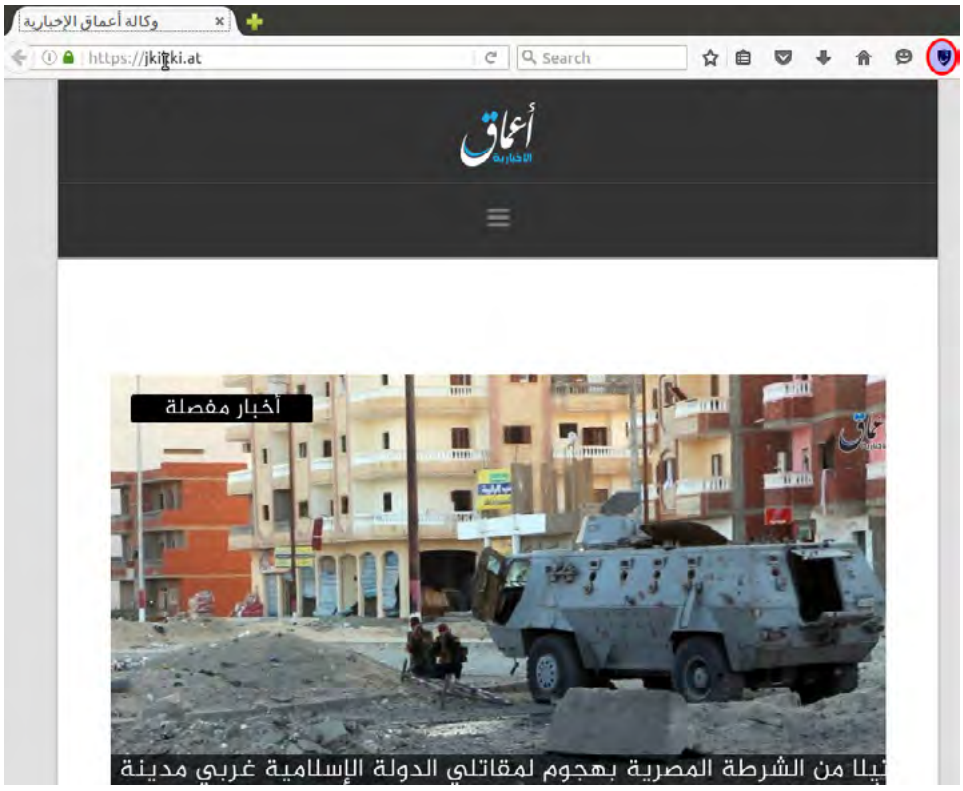
- install.rdf define, en el campo em:targetApplication, que la extensión está pensada para ser instalada en varias versiones. En este caso, explícitamente se muestra que es válida para diferentes versiones de Firefox, incluyendo Firefox para Android.

- lib/main.js contiene la lógica del complemento. La única diferencia entre la primera versión y la segunda es la dirección URL a la que enlazan.

EL USO DE LA EXTENSIÓN COMO MARCADOR

En el caso de la primera versión, la URL a la que apuntaba estaba alojada en una dirección que actualmente no se encuentra disponible pero vinculada a un proveedor de servicios de internet en Suecia. Sin embargo, la versión más reciente se encontraba vinculada (y activa en la fecha de la investigación) a un proveedor de servicios de hosting anónimo afincado en Panamá.

Esta última enlazaba a un sitio web protegido por Cloudflare en donde se almacenaba información sobre Amaq y el Estado Islámico. Al utilizar esta aproximación, bloquear el acceso al dominio en cuestión no sería suficiente para detener la propagación del contenido, ya que el desarrollador de la aplicación solamente tendría que ir modificando el campo Location de la redirección a un nuevo dominio en donde se alojara el nuevo contenido. Este es el matiz que le per-mitiría hacer perdurable el contenido en internet.



La estructura de la URL que aparecía en el campo Location sugería la posibilidad de la existencia de otros dominios. De esta manera, se pudieron identificar otros siete nuevos dominios afines empleando además del árabe, el alemán, el bengalí y el bosnio. Otro elemento significativo fue el uso de cuentas de correo cifradas para registrar los dominios.

RL	Dominio de redirección	Idioma	Certificado válido desd (aaaa/mm/dd)
:tp://190.14.37.220/b/	bibifm.at	árabe	2017/01/10
:tp://190.14.37.220/f/	vosn.pw	N/F	2016/01/06
:tp://190.14.37.220/g/	baqiya.ga	alemán	2017/01/01
:tp://190.14.37.220/h/	halummu.at	N/F	N/D
:tp://190.14.37.220/t/	nikmat.gq	bengalí	2017/01/10
:tp://190.14.37.220/u/	vijestiummeta.ga	bosnio	2017/01/05
:tp://190.14.37.220/v/	jkikki.at	árabe	2016/12/31

Identificación de otros dominios asociados

No es nuevo que Estado Islámico ha sabido adaptarse a la evolución tecnológica que vivimos. Ya ha demostrado en el pasado que ha sabido utilizar los medios a su alcance, como las redes sociales y las aplicaciones móviles para hacer llegar su mensaje. Sin embargo, en esta ocasión, ha tratado de ser más eficiente montando una infraestructura situada en diferentes países, usando Cloudflare como medida de protección o diversos servidores y métodos para garantizar la vigencia de su mensaje.

"la estrategia de Estado Islámico está evolucionando hacia el concepto de hacer perdurable su propaganda en Internet al margen de las acciones conjuntas de las grandes compañías tecnológicas"

3 Entrevista a Francisco Lázaro.
Responsable de Seguridad de la Información (CISO) de Renfe Operadora

1. Como responsable de seguridad de la información de la principal operadora ferroviaria de España, ¿podría indicarnos cuáles son sus principales competencias? ¿Cuál es su rol en la implementación de la estrategia corporativa?

Mis competencias son las del CISO del Grupo:

Definir la estrategia la seguridad de la información, establecer y velar por el cumplimiento de las políticas, gestionar los riesgos, proponer el Plan Director de Seguridad y gestionar su presupuesto.

Evaluar el Nivel de seguridad, monitorizar y supervisar el grado de seguridad que proporcionan los grupos de soporte, gestionar los incidentes de seguridad, realizar pruebas técnicas de verificación y Auditorías de cumplimiento,

Reporte a la alta Dirección, así como a organismos competentes, entre otras funciones.

El rol en la estrategia de Seguridad, y en consecuencia en su imbricación con la estrategia corporativa, es la identificar y proponer al Comité de Seguridad, para su posterior elevación a la Dirección, la estrategia, planes y proyectos que permitan apoyar los procesos de Negocio tanto operativos, como de transformación.

2. La coexistencia de sistemas informáticos corporativos junto con los sistemas de control industrial propios de una infraestructura ferroviaria, ¿supone un reto adicional desde el punto de vista de un gestor de riesgos de ciberseguridad? ¿Ambos entornos se encuentran expuestos a las mismas amenazas?

Como todos sabemos, cada elemento TI, ya sea corporativo, departamental, personal o industrial aumenta la exposición y la superficie de ataque y a su vez cada uno de estos entornos tiene sus particularidades, y condicionantes.

Los elementos SCADA son sistemas que han sido pensados para funcionar con seguridad industrial, en redes aisladas, basados en cumplir estándares y como todos los elementos de in-

Fuente: Renfe

fraestructura: instalados para durar años. Ahora, todos los sectores industriales, nos enfrentamos a la necesidad de proteger la evolución del ecosistema SCADA, el cual está cada vez más conectado y en consecuencia cada vez más susceptible de ser atacado. Sus vulnerabilidades y amenazas, pudiendo verlas como específicas, en realidad responden a los mismos vectores de siempre: Personas, Procesos y Tecnología. Sus riesgos deben ser analizados y gestionados de forma consistente y coherente, lo que implica por ejemplo entender la dificultad para seguir el ritmo de las actualizaciones y proceder de forma consecuente; implementando otro conjunto de medidas que nos permitan actuar eficazmente, contra la explotación de vulnerabilidades.

3. Como operador de una infraestructura crítica y en el complejo entorno de las empresas públicas, cuyos sistemas suelen estar amparados por normativas altamente restrictivas, ¿cómo balancea la necesidad de cumplir la normativa con las necesidades de protección real ante amenazas?

Efectivamente, todos los sectores críticos, y el del transporte no es diferente, por su propia naturaleza de prestadores de servicios esenciales tienen que cumplir con un conjunto amplio de obligaciones dadas por Normativas y Regulaciones.

Adicionalmente, las empresas públicas para garantizar una eficiente gestión de los recursos públicos deben garantizar en el proceso licitador de contratación de bienes y servicios la transparencia, igualdad y publicidad, lo que en principio pudiera parecer como una limitación para actuar con rapidez y confidencialidad, en la práctica no resulta serlo ya que lo compensamos con una mayor planificación, concreción de requisitos y manejo de información confidencial.

Así pues, el balanceo, es sencillo, pues en mi opinión no son extremos antagónicos, pues en materia de seguridad comparten los mismos objetivos. Consecuentemente la protección real ante amenazas debe realizarse desde el cumplimiento de normas y regulaciones, las cuales no son un obstáculo, sino que al establecer obliga-

ciones, estas deben ser vistas y tratadas como impulsoras de acciones.

4. El hecho de pertenecer a una entidad pública empresarial dependiente del Ministerio de Fomento, ¿hace más sencillo la coordinación de la seguridad con otros órganos estatales tales como INCIBE, CNPIC o el Centro Criptológico Nacional? ¿se facilita pues la lucha contra las amenazas digitales a través de los sistemas de protección de la propia Administración Pública?

La coordinación de la seguridad con INCIBE, CNPIC o CCN es constante y eficaz, no tanto por formar parte Renfe de la Administración General del Estado (AGE), sino por la implicación, apoyo, facilidades y profesionalidad que esos Organismos aportan tanto a los organismos públicos como a las empresas privadas.

La Administración pública, está impulsando decididamente la protección y la lucha contra las amenazas digitales , siendo un claro ejemplo el conjunto determinado por la Estrategia, la Ley y el Sistema de Seguridad Nacional.

5. ¿Considera que los mecanismos de compartición de información de amenazas existentes entre el sector público y el privado son eficaces? ¿Qué medidas propondría para fomentar dicho intercambio?

Todas las partes implicadas son conscientes de la necesidad de compartir información de amenazas y ataques; específicamente alertas e indicadores de ataque y compromiso (IOCs). No obstante, aún estamos muy lejos de alcanzar un nivel de adecuado de madurez en este campo.

Por ejemplo, todos los organismos disponen ya de nodos IOCs, generalmente conectados con CERTs y proveedores de inteligencia –típicamente fabricantes de seguridad y proveedores de servicio-, sin embargo fuera de ellos, su uso sólo está presente en las grandes empresas, su adopción es aún muy manual, y no llega a todos los activos que conforman la infraestructura de seguridad. Por otro lado, las empresas de seguridad que son parte importante en la ecuación no llevan muy bien eso de compartir, pues consideran que pierden oportunidades de negocio y comercialización de inteligencia.

"la protección real ante amenazas debe realizarse desde el cumplimiento de normas y regulaciones, las cuales no son un obstáculo, sino que al establecer obligaciones, estas deben ser vistas y tratadas como impulsoras de acciones."

Las medidas están ahí, ya existen protocolos y formatos, tecnologías que generan y consumen IOCs, iniciativas y acuerdos legales, pero aún queda lo más importante: que se hagan realidad y visibles iniciativas fuertes, integradoras, que combinen una gran cantidad de empresas "objetivo", organismos y proveedores de activos y servicios de seguridad.

Por eso quiero destacar, una nueva iniciativa del ISMS Forum que responde a todo lo que anteriormente he dicho. La iniciativa está en fase piloto y nace con siete empresas, entre las que

se encuentra Renfe. Estas empresas, a través de sus activos de seguridad (antimalware, cortafuegos, IDS, sondas, IPs, cajas de detonación, proxys avanzados, entre otros) y servicios CERTs, generan y consumen IOCs, los cuales son compartidos internamente y hacia el resto de los participantes mediante la unión de sus nodos MISP.

6. Ante la proliferación de los servicios de información de amenazas existente, ¿considera que las entidades que, como Renfe, deben gestionar tanto sistemas SCADA como sistemas IT tradicionales se encuentran en grado de llevar a cabo procesos de ciberinteligencia?

En la actualidad, no se concibe una eficaz gestión de los incidentes de seguridad sin ciberinteligencia, ya que esta inteligencia, no sólo debe ser sólo utilizada para descubrir brechas que han pasado desapercibidas o para anticiparse a situaciones de compromiso, sino también para aportar más información útil a la gestión de incidentes.

7. Dada su experiencia en el ámbito de la normalización relacionada con las evidencias electrónicas, ¿considera que disponemos del marco adecuado para el tratamiento y uso de las evidencias digitales admisibles procesalmente en España?

En los últimos seis años se han producido notables cambios tanto en el Ordenamiento Jurídico, como en la especialización de recursos. Dos claros ejemplos de ello son, tanto la creación en Octubre de 2011 de la figura del Fiscal de Sala de Criminalidad Informática, como más recientemente, la incorporación al código penal del delito "acceso ilícito a datos o programas" en su nueva redacción.

En el campo Normativo y de la estandarización, tanto las normas nacionales como las internaciones han aportado claridad y buenas prácticas.

Gracias a estos dos pilares (leyes y normas) tenemos un marco sólido. El problema de las evidencias radica en la naturaleza de las tecnologías de la información, en la complejidad y variedad de los elementos que intervienen en la

Fuente: Renfe

entrega de servicios, siendo por todo ello por lo que resulta complicada la detección, la correlación de registros, y la posterior demostración del mantenimiento durante todo el tiempo de la integridad y complitud de los eventos que serán aportados. Las acciones iniciales de investigación son necesarias para discernir si se trata de una incidencia, de un falso positivo, o de un incidente, y en este último caso, deberán haberse extremado los procedimientos y los cuidados para que en esos trabajos no se haya puesto en duda la autenticidad de la prueba. Finalmente, hay que hacer entendible en sede judicial lo que se presenta y lo que el atacante pretendía o con-siguió, y eso en muchos casos no es sencillo.

8. ¿Nos encontramos ante un escenario de indefensión ante el panorama de amenazas existente en la actualidad? ¿Qué recomendaciones generales propondría?

En mi opinión, el grado de indefensión de cada Organización viene dado fundamentalmente por su nivel de concienciación o incredulidad con el que se enfrenta a este nuevo panorama de ciberamenazas.

Las recomendaciones:

- Una Organización concienciada, sensibilizada y responsable en materia de Seguridad de la Información.
- Disponer (diseñar y desplegar) una estrategia adecuada de Seguridad, alineada con el Negocio (y este con la Seguridad).
- Valorar la información y gestionar eficazmente el riesgo.
- Rodearse de buenos profesionales.
- Aplicar el principio de seguridad y privaci-dad en el diseño.
- Gestionar eficientemente un presupuesto suficiente para disponer de buenos productos y servicios de seguridad.
- Fomentar y mantener la cooperación y la coordinación con terceros.
- Finalmente: una buena Gestión de Incidentes, crisis y continuidad.

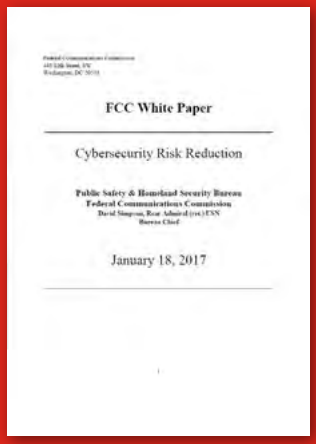
"el grado de indefensión de cada Organización viene dado fundamentalmente por su nivel de concienciación o incredulidad con el que se enfrenta a este nuevo panorama de ciberamenazas."

4 Informes y análisis sobre ciberseguridad publicados en enero de 2017

Report on Cyber Security Information Sharing in the Energy Sector (ENISA)

A good practice guide of using taxonomies in incident prevention and detection (ENISA)

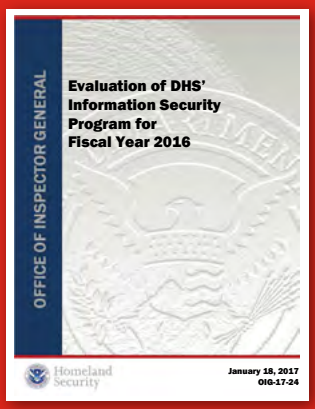
Cyber Security Risk Reduction (U.S Department of Transportation)



Assessing Russian Activities and Intentions in Recent US Elections (U.S ODNI)

Blockchain in the Insurance Sector (McKinsey)

Evaluation of DHS´Information Security program for FY2016 (DHS)



2017 Cyber Threats (Fireeye)

Cyber, Intelligence and Security (INSS)

5 HERRAMIENTAS DEL ANALISTA:
Ikanow

IKANOW es una compañía estadounidense de análisis de datos basada en Reston, Virginia, cuyas soluciones recolectan y analizan grandes volúmenes de datos estructurados y no estructurados. Fundada en 2010, IKANOW creó una plataforma de análisis utilizando tecnologías de código abierto. También realiza análisis de amenazas para ayudar a las organizaciones a evaluar sus niveles de riesgo actuales, mejorar el nivel seguridad y aumentar la conciencia situacional.

La version gratuita de su solución, denominada IKANOW Community Edition, antes llamada Infinite.e, ha sido empleada para realizer análisis de sentimiento sobre la base de datos de emails de la investigación realizada por la *Federal Energy Regulatory Commission* sobre el caso *Enron*.

IKANOW permite sacar el máximo valor a los datos existentes, ya sean estructurados o no. Esta potente herramienta de análisis de seguridad de código abierto ofrece mecanismos de ingesta de última generación, búsqueda avanzada, útiles widgets de datos y funciones de exportación para compartir la información. Se integra con aplicaciones de terceros para proporcionar una solución completa de código abierto para el análisis masivo de datos. La Community Edition tiene incorporados los conectores que permiten las integraciones con OpenNLP, Stanford, UIMA, y otros incluyendo OpenCalais y AlchemyAPI.

Los principales elementos de la solución son:

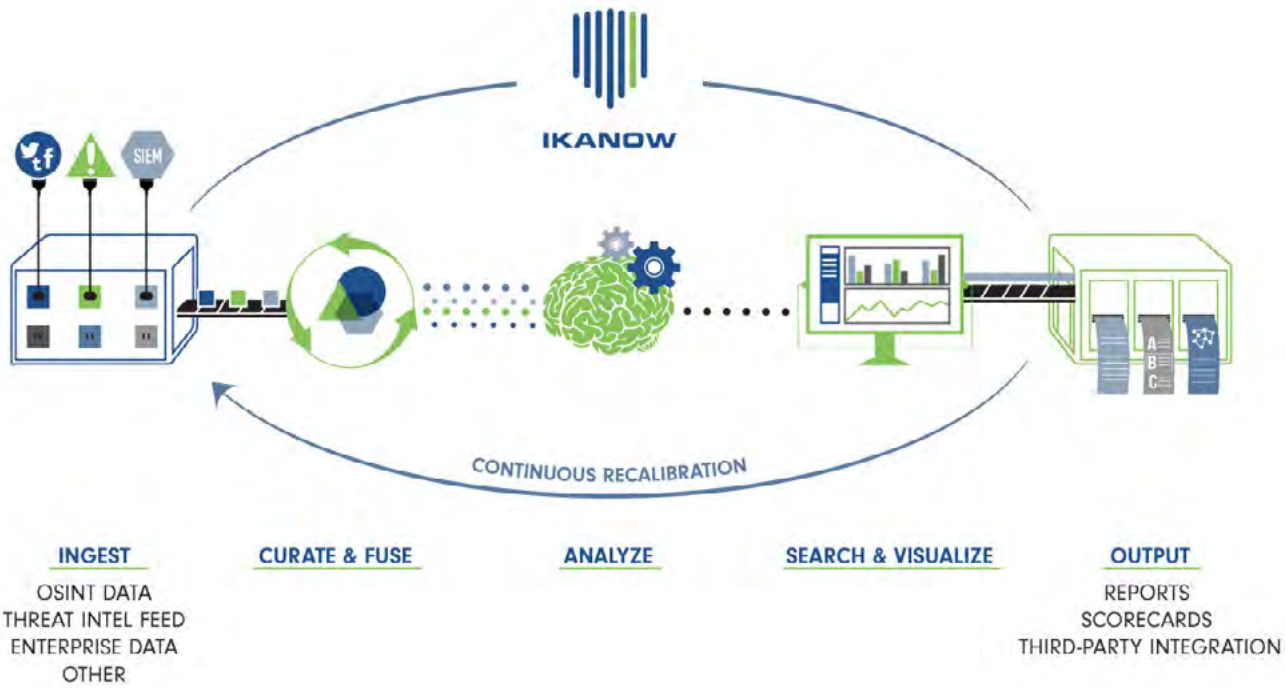
- IKANOW Engine: motor principal de la plataforma que emplea tecnologías como MongoDB, elasaticsearch y Hadoop.

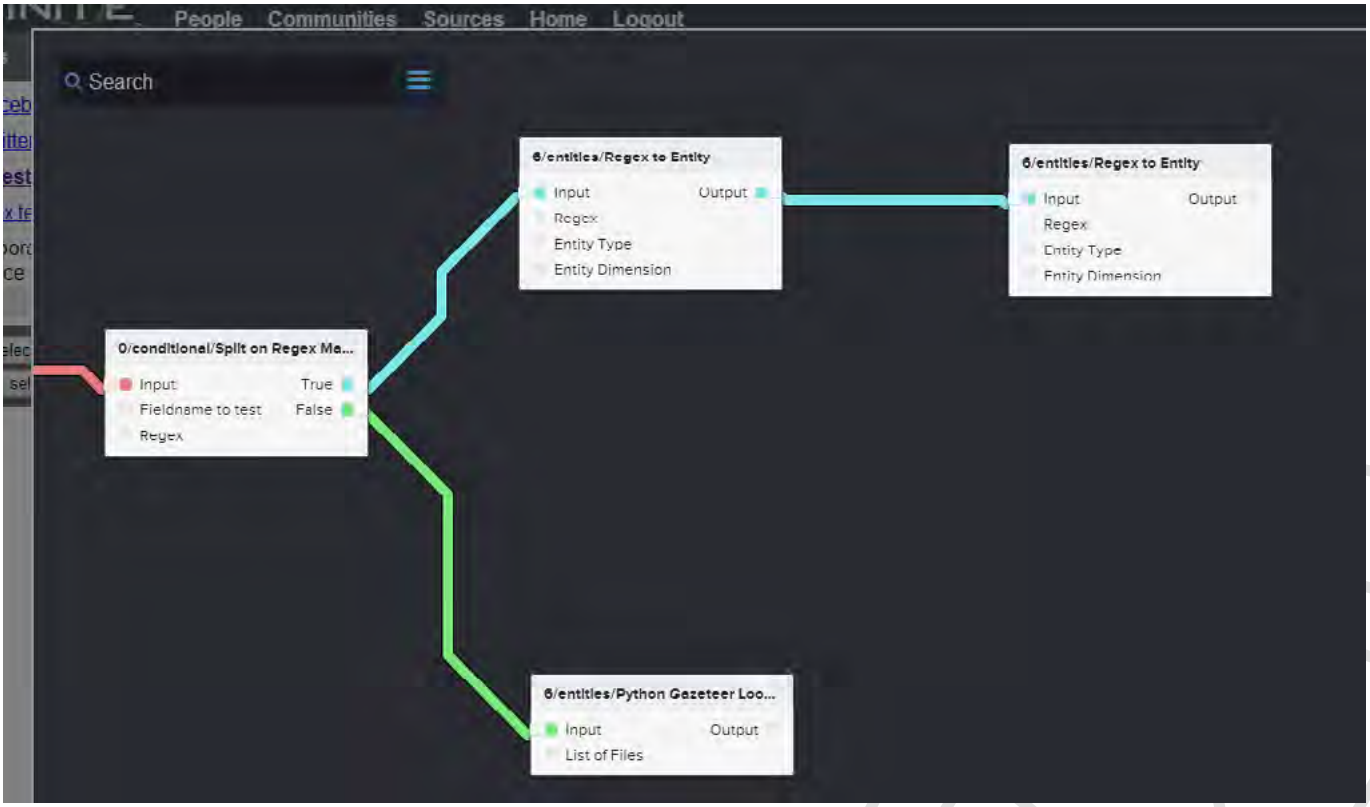
- IKANOW View: capa de presentación que cuenta con diversos plugins para representar los datos.

- IKANOW Toolkit: incluyendo herramientas de análisis, *widgets* de visualización: *Mapas*, IKANOW Browser, *Timeline* de eventos, *grafo de evento*, *métricas*, análisis de sentimiento, etc.

- IKANOW EnrichmentData: motores de enriquecimiento de datos , extractores de entidades (Text Rank, OpenCalais, AlchemyAPI) y extractores de texto (Boilerpipe, Tika, AlchemyAPI) así como Plugins personalizados.

- IKANOW Manager.


IKANOW
SIEM
CONTINUOUS RECALIBRATION
INGEST
OSINT DATA
THREAT INTEL FEED
ENTERPRISE DATA
OTHER
CURATE & FUSE
ANALYZE
SEARCH & VISUALIZE
OUTPUT
REPORTS
SCORECARDS
THIRD-PARTY INTEGRATION


People
Communities
Sources
Home
Logout
Search
6/entities/Regex to Entity
Input
Output
Regex
Entity Type
Entity Dimension
6/entities/Regex to Entity
Input
Output
Regex
Entity Type
Entity Dimension
0/conditional/Split on Regex Ma...
Input
True
Fieldname to test
False
Regex
6/entities/Python Gazeteer Loo...
Input
Output
List of Files

6 Análisis de los Ciberataques del mes de enero de 2017

AUTOR: Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank.
Cybersecurity advisor, Telefonica/ElevenPaths.

CIBERCRIMEN

A finales de diciembre de 2016, aprovechando aparentemente una vulnerabilidad de día 0 del gestor de contenidos Plone CMS, un atacante denominado *CyberZeist afirma haber sustraído información confidencial del portal FBI.GOV* publicando registros de 155 funcionarios del FBI en la plataforma *pastebin*.

Tweet de CyberZeist anunciando el hackeo a la web FBI.GOV

Ya mediados de enero, el regulador bancario indio anunció la presencia de *actividad anómala en los sistemas de tres bancos estatales* -dos de ellos con sede en Mumbai y otro en Kolkata- cuyo resultado fue la creación de falsos documentos comerciales que podrían haber sido usados para recaudar fondos en el extranjero o facilitar negociaciones con información privilegiada.

Los bancos en cuestión descubrieron que sus sistemas SWIFT fueron comprometidos, creando los mencionados documentos. Los bancos todavía no están seguros sobre el origen del ataque y la motivación de los atacantes.

El 12 de enero, Cellebrite, la compañía israelí cuyo principal producto, el denominado Universal Forensic Extraction Device (UFED), permite extraer datos de miles de modelos diferentes de teléfonos móviles, ha sido atacada. Entre los datos que UFED puede obtener de un dispositivo móvil se incluyen mensajes SMS, correos electrónicos, registros de llamadas y mucho más, siempre y cuando el usuario de UFED esté en posesión del teléfono físicamente.

Como resultado del ataque, más de 900 GB de datos de la compañía han sido hechos públicos. La fuga de datos incluye información de clientes, bases de datos y una gran cantidad de datos técnicos sobre los productos corporativos.

Esta fuga es el último capítulo en una creciente tendencia que muestra como las empresas que se especializan en la vigilancia en internet o tecnologías de seguridad ofensiva son víctimas habituales de los cibercriminales.

CIBERESPIONAJE

El *Centro Nacional Británico de Ciberseguridad (NCSC por sus siglas en inglés)* reveló a comienzos de año *haber frustrado cerca de 86 ataques en su primer mes de actividad* tras ser inaugurado en octubre de 2016. La mayoría de los ataques parecen provenir de China, Corea del Norte, Rusia, Irán y grupos criminales

organizados. Los principales objetivos atacados han sido el Banco de Inglaterra, el Ministerio de Defensa, bases nucleares, servicios de seguridad y grandes infraestructuras como la red de transporte, el NHS y los sistemas de distribución de energía.

National Cyber Security Centre
a part of GCHQ

El 11 de enero, los hermanos italianos Giulio Occhionero y Francesca Maria Occhionero fueron *arrestados en Roma acusados de llevar a cabo una larga campaña de ciberespionaje contra los principales políticos, empresarios y masones italianos.*

El malware supuestamente utilizado por ambos es conocido como *EyePyramid*, posiblemente haciendo referencia al Ojo de la Providencia que se encuentra en el billete de un dólar de los Estados Unidos y a menudo asociado con la francmasonería. Los investigadores creen que la operación puede haber estado funcionando desde el año 2010.

Giulio Occhionero es un miembro de alto rango de la logia masónica Grand Orients, y fue presuntamente preseleccionado como Maestro Masón. Según la orden de arresto, uno de sus objetivos era el gran maestro de la mayor logia de Italia, siendo fácil inferir algún tipo de implicación masónica el caso.

No hay, sin embargo, evidencia clara de la motivación tras la campaña, ni la cantidad o calidad exacta de los datos robados. Los datos extraídos fueron enviados y almacenados en servidores en Estados Unidos, uno en Prior Lake, Minnesota, y el otro en Salt Lake City, Utah. El FBI colaboró con las autoridades italianas en la operación, incautando los dos servidores y enviándolos a Italia para su análisis.

El contenido no se conocerá hasta que los servidores hayan sido completamente examinados en Italia. Sin embargo, Roberto Di Legami, jefe de la unidad cibernética especializada de la policía que llevó a cabo la investigación italiana, dijo que Occhionero "era muy obsesivo en catalogar la información". La información robada fue cuidadosamente archivada en más de 120 categorías, incluyendo una carpeta llamada 'BROS' que contenía correos electrónicos relacionados con una logia masónica, y otra con respecto a los políticos fue nombrada 'POBU' para Políticos de Negocios. Se cree que se almacenan hasta 87Gb de datos.

Según la orden de arresto, el presidente del Banco Central Europeo, Mario Draghi, y dos ex primeros ministros italianos, Matteo Renzi y Mario Monti, estuvieron entre las víctimas. En total, parece que más de 18.000 cuentas de correo electrónico pueden haberse comprometido. No se cree que la cuenta de ECB de Draghi haya sido comprometida y no hay pruebas de que alguna cuenta del BCE se haya visto comprometida.

El equipo de analistas de TrendMicro ha publicado un par de análisis sobre el *malware empleado* y *el vector de ataque.*

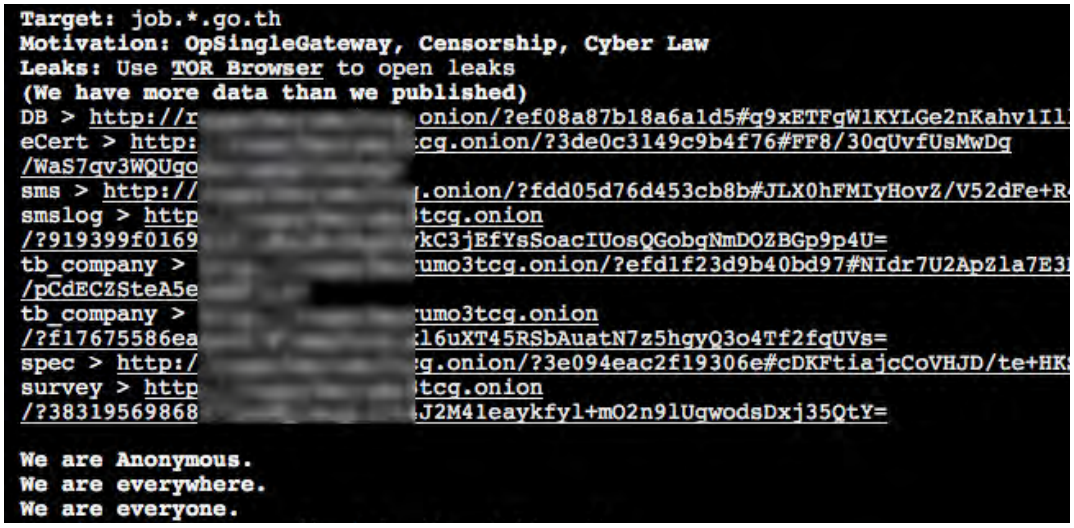
The domains being targeted				
@alice.it	@gmail.com	@katamail.com	@orange.fr	@wanadoo.fr
@aol.com	**@gmail.it**	@laposte.net	@otenet.gr	@web.de
@att.net	@gmx.de	@legalmail.it	@poczta.onet.pl	@yahoo.ca
@badoo.com	@gmx.net	@libero.it	@poste.it	@yahoo.co.in
@bellsouth.net	@googlegroups.com	@live.com	@proxad.net	@yahoo.co.jp
@bluewin.ch	@googlemail.com	@live.it	@rediffmail.com	@yahoo.co.uk
@btinternet.com	@groupama.it	@lycos.com	@rocketmail.com	@yahoo.com
@comcast.net	@groups.facebook.com	@lycos.it	@runbox.com	@yahoo.com.ar
@cox.net	@gvt.net.br	@mac.com	@saudi.net.sa	@yahoo.com.br
@cyh.com.tr	@hanmail.net	@mail.bakeca.it	@sbcglobal.net	@yahoo.com.mx
@earthlink.net	@hinet.net	@mail.com	@skynet.be	@yahoo.de
@eim.ae	@hotmail.co.uk	@mail.ru	@supereva.it	@yahoo.es
@email.com	@hotmail.com	@mail.vodafone.it	@sympatico.ca	@yahoo.fr
@email.it	@hotmail.fr	@mail.wind.it	@t-online.de	@yahoo.it
@emirates.net.ae	@hotmail.it	@mclink.it	@tele2.it	@yahoogroups.com
@excite.it	@infinito.it	@me.com	@verizon.net	@ymail.com
@facebook.com	@interbusiness.it	@msn.com	@virgilio.it	
@facebookmail.com	@interfree.it	@mtnl.net.in	@vodafone.com	
@fastweb.it	@inwind.it	@nate.com	@vodafone.it	
@fastwebmail.it	@iol.it	@netscape.net	@vsnl.net.in	
@fastwebnet.it	@jazztel.es	@netzero.com		
@free.fr	@jumpy.it			

Dominios de email atacados

El grupo *hacktivista Anonymous ha llevado a cabo otra campaña de ataques contra objetivos del gobierno de Tailandia* como protesta tras la recientemente aprobada ley de ciber-escrutinio, bajo la operación #OpSingleGateway. Esta vez el grupo se ha centrado en el portal de empleo del gobierno tailandés, provocando la fuga de datos personales y sensibles de los funcionarios y solicitantes de empleo.

Los datos que se han filtrado en la darkweb se han dividido en varios foros y markets , incluyendo las diversas bases de datos del portal, nombres, apellidos, nombres de las empresas asociadas, detalles de pago, números de teléfono, números de cuenta bancaria, correos electrónicos y contraseñas cifradas.

El dominio atacado por Anonymous es job.*. go.th. En este caso, los datos han sido robados del Departamento de Ingresos, del Tribunal Administrativo, del Departamento de Bellas Artes, del Departamento de Auditoría Cooperativa, de la Autoridad Provincial de Obras Hidráulicas, de la Oficina de Gestión de la Deuda Pública, del Departamento de Parques Nacionales, la tecnología de las comunicaciones, el Ministerio de Re-laciones Exteriores y varios otros departamentos del gobierno tailandés.



Captura de pantalla mostrando un extracto de los datos filtrados en un sitio de la darkweb

A mediados de mes se conocía el *ataque perpetrado por el experto en seguridad conocido como Kapustkiy sobre el Gobierno de Venezuela*, filtrando datos en *Pastebin.* Kapustkiy hackeó el sitio web *www.gdc.gob.ve* mediante la explotación de una vulnerabilidad de Inclusión de archivos locales (LFI) en la dirección web Http://www.gdc.gob.ve/2.0/gui_resources/css/?f=../../../../../../../../../ .. / Etc / passwd.

Según comunicó el propio autor, había encontrado un LFI en el sitio web de la capital del gobierno de Venezuela, hackeando también otros dos sitios web mediante la explotación de una inyección SQL, encontrando alrededor de 800 usuarios en éstos últimos. El hacker realizó este ataque en protesta contra el presidente de Venezuela, explicando que está destruyendo la vida de sus conciudadanos con sus medidas políticas.

7 Recomendaciones

7.1 Libros y películas

Película:
PASSENGERS

Sinopsis: Una nave espacial, que viaja a un planeta lejano transportando a miles de personas, tiene una avería en una de las cápsulas de hibernación tras el impacto con un gran meteorito. Como resultado, un pasajero se despierta noventa años antes del final del viaje.

Libro:
BITCOIN: LA TECNOLOGÍA BLOCKCHAIN Y SU INVESTIGACIÓN

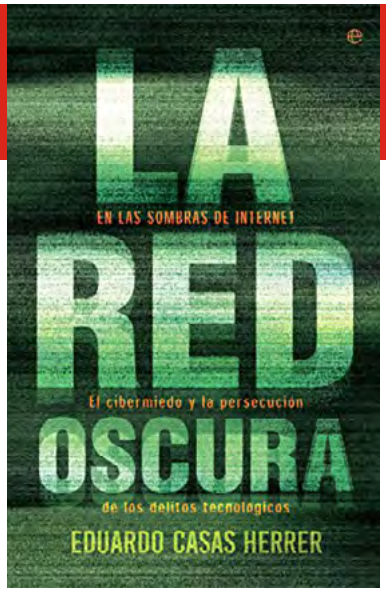
Autor: Felix Brezo y Yaiza Rubio
Num. Paginas: 208
Editorial: 0xWORD
Año: 2017
Precio: 22.00 Euros
Sinopsis: ¿Cuánto vale un bitcoin? ¿Dónde puedo conseguirlos? ¿Hasta qué punto es anónimo el pago con bitcoins? ¿Y si los pierdo? ¿Puedo crearme mi propia criptodivisa? ¿Qué cosas puedo adquirir o comprar? ¿Qué puedo saber de una dirección y hasta dónde puedo rastrearla? ¿De verdad la tecnología de Blockchain solucionará todos mis problemas? A estas y otras preguntas se darán respuesta en las páginas de este libro desde un punto de vista práctico y con el apoyo de las tecnologías libres que han hecho posible el desarrollo de una comunidad que va mucho más allá del sistema de pago descentralizado que empezó a incubar un aún desconocido Satoshi Nakamoto.

Libro:
EL LADO OSCURO DE LA RED

Autor: Misha Glenny
Num. Paginas: 286
Editorial: Destino
Año: 2014
Precio: 15.00 Euros
Sinopsis: Misha Glenny, escarba con determinación en la trastienda del cibercrimen a partir del auge y la desaparición de la web Dark Market, dedicada a la compra y venta de datos bancarios de ciudadanos de todo el mundo entre 2005 y 2008. Tras recorrer medio mundo y entrevistarse con criminales, policías, víctimas y hackers, Glenny desvela en este ensayo con aroma a thriller todos los secretos de la floreciente industria del cibercrimen, denuncia la insuficiencia de los medios policiales y la escasa implicación de las instituciones bancarias y, por encima de todo, plantea interrogantes sobre la seguridad en los tiempos de internet, convirtiendo "El lado oscuro de la red" en una lectura obligatoria para cualquiera que utilice un ordenador en nuestros días.

Libro:
CIBERDICCIONARIO

Autor: Javier Zubieta
Editorial: Javier Zubieta (Kindle Edition)
Año: 2015
Precio: 4.00 Euros
Sinopsis: El Ciberdiccionario es una recopilación de conceptos de Ciberseguridad explicados en un lenguaje llano, asumiendo que el lector dispone de conocimientos técnicos básicos o incluso nulos. El objetivo es hacer entendible unos conceptos que en general son más sencillos de lo que parecen a primera vista.



Libro:
LA RED OSCURA

Autor: Eduardo Casas
Num. Paginas: 336
Editorial: La Esfera de los libros
Año: 2017
Precio: 22.00 Euros
Sinopsis: No solemos pararnos a pensar cómo funciona un motor de búsqueda de Internet, y es precisamente en su manera de actuar donde se encuentra su punto débil: la araña. Por mucho que se esfuerce el robot, hay lugares a los que no es capaz de llegar porque no está diseñado para ello. Y de esa red oscura a la que no puede acceder solo es visible el uno por ciento, el resto está escondido, como si de un iceberg se tratara. Negocios ilegales, tráfico de armas y de productos, muertes retransmitidas, pornografía infantil… conforman el lado negativo de Internet; un pozo sin fondo que se abre desde nuestras pantallas. El autor de este libro, miembro del Cuerpo Nacional de Policía, que lleva desde 2004 trabajando en la Brigada de Investigación Tecnológica (BIT), nos explica con notable claridad cómo persiguen sin tregua y sacan a la luz los delitos de ese universo desconocido de la red.

7.2 Webs recomendadas

http://www.inss.org.il/index.aspx?id=4438
Sitio web de la sección ciberseguridad del Instituto de Estudios de Seguridad Nacional de Israel (INSS).

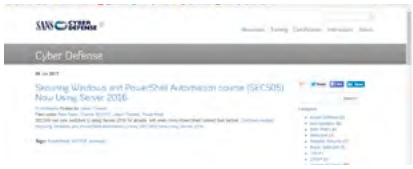
http://www.usma.edu/acc/SitePages/Home.aspx
Sitio web del Instituto de Ciberseguridad del U.S Army en West Point.

http://blog.ioactive.com/
Blog de la compañía de ciberseguridad IO Active

https://paulcsfi.wordpress.com/
Blog de Paul de Souza, fundador del Cyber Security Forum Initiative (CSFI)

https://cyber-defense.sans.org/blog/
Sitio web de SANS dedicado a la ciberdefensa

https://www.ncsc.gov.uk/blog
Blog del Centro Nacional de CiberSeguridad del gobierno británico.



7.3 Cuentas de Twitter

@thorsheim

@HeadLeaks

@yadox

@yrubiosec

@BnkInfoSecurity

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
6- 7 Febrero	Dubai	QATALYST GLOBAL	Industrial Internet of Things MENA	https://www.industrialiotseries.com/mena-attendee-list/
6- 7 Febrero	Dubai	Fleming	Cyber Resilience & InfoSec 2017	https://fleming.events/en/events/security/cyber-resilience-infosec
6- 7 Febrero	Cambridge, UK	UNICRI	The Risks and Benefits of Artificial Intelligence and Robotics	http://unicri.it/services/education_training/journalism_public_information_programme/artificial_intelligence/
13- 17 Febrero	San Francisco	RSA	RSA Conference USA	https://www.rsaconference.com/events/us17
15-17 Febrero	Londres	IQPC	Big Data Analytics For Insurance	https://dataanalyticsinsurance.iqpc.co.uk/
15 Febrero	San Francisco	OASIS	Using Stix/taxii To Share Automated Cyber Threat Data	https://www.eventbrite.com/e/using-stixtaxii-to-share-automated-cyber-threat-data-tickets-30962683219
15-17 Febrero	Berlín	IT- Defense	IT-Defense 2017	https://www.it-defense.de/
19- 21 Febrero	Oporto	ICISSP	3rd International Conference on Information Systems Security and Privacy – ICISSP 2017	http://www.icissp.org/
21 Febrero	Dubai	New Banking	FinSec - The Banking/ Financial Cybersecurity Summit 2017	http://newagebanking.com/finsec
21-22 Febrero	Londres	Business Reporter	European Information Security Summit 2017 (TEISS)	https://biztechevents.co.uk/teiss/
23 Febrero	Tenerife	Hackron	Hackron	http://www.hackron.com/
24 Febrero	Escocia	Ethical Hacking Society at Abertay University	Securi-Tay 2017	https://2017.securi-tay.co.uk/

Patrocinadores

GOBIERNO DE ESPAÑA — MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

GOBIERNO DE ESPAÑA — MINISTERIO DE DEFENSA

GOBIERNO DE ESPAÑA — MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

GOBIERNO DE ESPAÑA — MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

ACERINOX · AIRBUS GROUP · ATLANTIC COPPER · BBVA

enagas · IBERDROLA · IBM · INDITEX

indra · CaixaBank · MUTUAMADRILEÑA · OHL

RED ELÉCTRICA DE ESPAÑA · renfe · REPSOL

Santander · Telefónica

Consejo Asesor Empresarial

CAF BANCO DE DESARROLLO DE AMÉRICA LATINA · endesa

IBERIA · Fundación Cajasol

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269