MAYO 2016 / Nº 14

CIBER elcano

REAL INSTITUTO elcano ROYAL INSTITUTE

Desarrollado por:

THIBER

INFORME MENSUAL DE CIBERSEGURIDAD

REAL INSTITUTO
elcano
ROYAL INSTITUTE

Copyright y derechos:

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
Reino Unido: la necesidad de consolidar el Sistema Nacional de Ciberseguridad

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

Cuartel general del GCHQ. Fuente:Reuters

En Noviembre de 2011, el gobierno británico aprobaba su *Estrategia Nacional de Ciberseguidad*, un documento programático que giraba en torno a cuatro grandes objetivos:

- Luchar contra el cibercrimen y convertir al Reino Unido en el lugar más seguro del mundo para hacer negocios en el ciberespacio.
- Mejorar las cibercapacidades defensivas del país.
- Trabajar en el desarrollo de un ciberespacio lo más abierto y estable posible.
- Generar los conocimientos, habilidades y capacidades que necesita el Sistema Nacional de Ciberseguridad del país para su desarrollo.

Tras cuatro años, un exhaustivo plan de implementación y casi 1.000 millones de Euros invertidos, el gobierno de Cameron hace un balance positivo de los logros alcanzados tras la implementación de la primera Estrategia de Ciberseguridad Nacional. Sin embargo, también reconoce que esta inversión no ha sido suficiente. En consecuencia, se espera que en los próximos meses el gobierno de Londres apruebe y haga pública la segunda Estrategia Nacional de Ciberseguridad que, partiendo de los hitos alcanzados por la primera, contará con un presupuesto aproximado de 2.500 millones de Euros para consolidar el incipiente Sistema Nacional de Ciberseguridad.

Uno de los principales objetivos de la nueva estrategia será seguir potenciando la Industria Nacional de Ciberseguridad, tan necesaria para consolidar los objetivos de la presente y futura estrategias. En la actualidad, la industria británica de ciberseguridad tiene un volumen de negocio superior a los 19.000 millones de Euros – por los 11.000 millones estimados en 2011- y ha generado más de 100.000 empleos directos. Además, se estima que ochenta empresas del sector ofrecen servicios y productos al gobierno británico. Del mismo modo, el sector nacional de la ciberseguridad ha incrementado en un 35% las exportaciones desde 2012 hasta alcanzar la cifra de 1.700 millones de euros, estimándose que podría alcanzar los 2.000 millones de Euros a finales de 2016.

Del mismo modo, el gobierno de Londres deberá seguir potenciando la educación y concienciación en materia de ciberseguridad. En este sentido, más de 23.000 estudiantes de ochocientas escuelas del país ya han recibido formación en materia de ciberseguridad. En los próximos años se prevé la potenciación de la educación en el ámbito universitario apoyándose en los Centros de Excelencia en Ciberseguridad y la creación de programas de doctorado en esta materia. Además, 77.000 ciudadanos han superado con éxito el *programa CyberEssentials.*

Finalmente, el Reino Unido aspira a seguir siendo un referente mundial en el impulso de la cooperación internacional en materia de ciberseguridad. Precisamente, en 2011 Londres acogió la primera *Conferencia Global sobre el Ciberespacio* que cada año se celebra en un país del mundo.

En otras palabras, en 2011 el Reino Unido comenzó su andadura para construir un Sistema Nacional de Ciberseguridad seguro, resiliente y competitivo. Aunque su construcción finalizará en los próximos años a medida que se consoliden las líneas trazadas en la Estrategia de Ciberseguridad Nacional, parece evidente que la potenciación de su industria nacional de ciberseguridad ha sido, es y será uno de los principales activos en este proceso. Sin una Industria Nacional de Ciberseguridad de primer nivel no es posible la construcción de un Sistema Nacional de Ciberseguridad. Muchos países deberían tomar cuenta de ello.

"Sin una Industria Nacional de Ciberseguridad de primer nivel no es posible la construcción de un Sistema Nacional de Ciberseguridad."

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL
Ciberseguros: un mercado en auge en España

AUTORES: Ángel Vallejo. Responsable de Relaciones Institucionales, THIBER.
Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank.
Cybersecurity advisor, Eleven Paths (Telefónica).

Desde sus inicios en la década de 1990, el mercado de los ciberseguros – definidos éstos como productos aseguradores cuyo objetivo es proveer protección ante una amplia gama de incidentes derivados de los riesgos en el ciberespacio, el uso de infraestructuras tecnológicas y las actividades desarrolladas en este entorno – ha ido penetrando lenta pero decididamente en el tejido industrial estadounidense y europeo. Con un número creciente de proveedores, una cadena de valor cada vez más madura y consolidada, un volumen de negocio en continuo auge y un aumento de la oferta y la competencia en el sector, los ciberseguros se han convertido en un producto cada vez más popular.

En España, con un volumen de negocio que ronda los 500 millones de euros anuales y un crecimiento anual del 12%, el mercado de los ciberseguros se halla en proceso de expansión. Hasta hace escasos años, éste se había centrado en productos dirigidos a las grandes empresas debido a su mayor exposición a los riesgos cibernéticos. No obstante, en la actualidad este mercado se orienta además al sector de la pequeña y mediana empresa – con una limitada experiencia en la gestión de estos riesgos, una creciente exposición a los ciberataques y, sobre todo, una necesidad de cumplir con un marco regulatorio cada vez más exigente en materia de protección de datos – adaptando su oferta a su realidad específica y necesidades concretas.

En consecuencia, tal y como ha analizado recientemente THIBER en su estudio *'Ciberseguros: la transferencia del ciberriesgo en España'*, los ciberseguros no sólo permiten transferir el riesgo corporativo a terceros, sino que también promueven la adopción de medidas de ciberprotección más robustas y mejorar la ciberseguridad del mercado, puesto que pueden requerir a sus clientes el cumplimiento de unas cautelas mínimas de ciberseguridad como condición sine qua non para la contratación de las pólizas; ofrecer descuentos en las primas a aquellas entidades que demuestren un nivel adecuado de madurez en seguridad; poner en práctica los procedimientos de gestión de ciberincidentes en nombre del asegurado; comprender los patrones de las amenazas y mejorar el intercambio de información entre el gobierno y las empresas aseguradas respecto a ciberincidentes proporcionando una alerta temprana ante este tipo de incidentes.

Un mercado de ciberseguros consolidado deberá desempeñar un papel protagonista en la economía española porque permitirá al asegurado trasladar los riesgos de su actividad a un tercero con capacidad económica para soportarlos; además, reforzará la posición crediticia del asegurado y fomentará la inversión productiva y el ahorro.

Aunque el mercado nacional de los ciberseguros es netamente privado, para incentivar su adopción deberán crearse unas líneas de acción desde los organismos gubernamentales de forma que se reduzca el coste de las primas mediante la asunción de parte de las coberturas de las aseguradoras privadas a través de programas de reaseguro. Igualmente, cuando los riesgos sean considerados como "no asegurables" por el mercado asegurador privado, el Estado debería asumir ciertos riesgos para reemplazar o estabilizar el mercado privado mediante programas específicos de compensación. En tercer lugar, será fundamental promover la adopción de marcos de ciberseguridad con un nivel de madurez determinado como una muestra de control debido, siendo de esta forma condiciones atenuantes ante potenciales y limitando por extensión las responsabilidades civiles e, incluso, penales según la legislación nacional. Al mismo tiempo, teniendo en cuenta que la propia Administración Pública española posee un nutrido ecosistema de proveedores de Tecnologías de la Información y de las Comunicaciones, se recomienda que actúe como eje vertebrador para aumentar el nivel de resiliencia de todos sus proveedores en términos de ciberseguridad y, por extensión, de un alto porcentaje del tejido empresarial nacional. Finalmente, el Estado puede favorecer el establecimiento de unos criterios comunes de seguridad a través de un marco de controles de seguridad de referencia cuya observancia y cumplimiento por parte de las empresas facilitase al sector asegurador la suscripción de seguros de ciberriesgos.

El mercado de los ciberseguros en España es un mercado en auge. Es responsabilidad de todos los actores garantizar su consolidación (publicado en elespanol.com el 05 de mayo de 2016).

3 Entrevista a Gianluca D'Antonio.

Presidente de ISMS Forum Spain.

1. Actualmente preside la asociación ISMS Forum Spain, ¿nos podría explicar cuáles son las principales líneas de acción de la asociación?

La Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, se encuentra ya cerca de su décimo aniversario y, a día de hoy, se consolida con más de 900 asociados y 150 empresas como la principal asociación en torno a la seguridad de la información en España. Cuenta con diferentes iniciativas que abarcan los que podemos denominar los principales "dominios" de la seguridad lógica, la privacidad y la protección de datos en entornos profesionales, como son el Cyber Security Centre (CSC), el Data Privacy Institute (DPI), el Centro de Estudios en Movilidad e Internet de las Cosas, o el capítulo español de Cloud Security Alliance España (CSA ES). Asimismo mantiene una línea de formación puntera y una certificación propia en torno a la especialización en protección de datos, el Certified Data Privacy Professional (CDPP), que cuenta ya con más de 160 profesionales certificados. No menos importante es la concienciación a todos los niveles, por lo que la Asociación gestiona el portal para ciudadanos www.protegetuinformacion.com.

Sin duda, uno de los proyectos más relevantes en la trayectoria de la Asociación ha sido la realización de ciberejercicios en el sector privado para la mejora de la resiliencia empresarial. Iniciativa pionera a escala nacional

que ha contado con el apoyo y el impulso de las principales compañías e instituciones en España y que hoy prepara ya su quinta edición.

2. A finales de 2013, el gobierno aprobó la Estrategia Nacional de Ciberseguridad, ¿qué balance hace del desarrollo de la citada estrategia? ¿Qué medidas propondría para mejorar el actual Sistema Nacional de Ciberseguridad?

No cabe duda que desde la aprobación de la Estrategia Nacional de Ciberseguridad el país en su conjunto ha mejorado en lo referente a concienciación acerca de la importancia de la ciberseguridad como un aspecto crítico de la sociedad. Seguimos en la senda del desarrollo de capacidades de respuesta a las amenazas del ciberespacio en todas las organizaciones. Es un proceso de madurez que conlleva tiempo y recursos. La aprobación de la estrategia ha tenido como efecto principal el de formalizar

los objetivos, definir las directrices y marcar los pasos a través de los cuales la sociedad española en su conjunto debe ir preparándose para hacer frente a los desafíos de las nuevas tecnologías. Mirando a otros países y experiencias en esta materia, quizá podemos incrementar el nivel de colaboración público-privada con una mayor involucración de los actores privados en la toma de decisión acerca de las prioridades y directrices en lo referente a ciberseguridad. Experiencias como los ciberejercicios del sector privado son elementos de capacitación fundamentales para mejorar de forma gradual la resiliencia de nuestras organizaciones.

"desde la aprobación de la Estrategia Nacional de Ciberseguridad el país en su conjunto ha mejorado en lo referente a concienciación acerca de la importancia de la ciberseguridad como un aspecto crítico de la sociedad.

3. En su opinión, ¿cuáles son los principales retos en materia de ciberseguridad que deberemos afrontar como país en los próximos 5 años?

Creo que tanto España como cualquier otra economía avanzada deberá hacer frente a tres retos principales:

1. El gobierno del Internet de las Cosas en las diferentes vertientes de seguridad: regulación, calidad de producto, régimen de la responsabilidad, concienciación y capacitación del usuario final del producto.
2. Introducir una educación básica en todos los niveles de la sociedad acerca de las ciberamenazas.
3. Tratar la ciberseguridad como un bien público.

4. Recientemente THIBER ha presentado un estudio sobre ciberseguros, ¿considera que los ciberseguros son la última línea de defensa contra las amenazas cibernéticas?

La entrada de las empresas aseguradoras en el ecosistema de los actores de la ciberseguridad, sin lugar a dudas, beneficia a todos los actores por la capacidad de estas empresas de desarrollar modelos de cálculo y gestión del riesgos que necesitamos todos los que trabajamos en este ámbito. Los ciberseguros pueden ser un complemento eficaz en la gestión del riesgo ciber para las empresas con cierta exposición a este tipo de amenazas.

5. En 2015, ISMS Forum Spain y THIBER propusieron al gobierno un conjunto de incentivos públicos para la mejora de la ciberseguridad nacional. En su opinion, ¿qué incentivos públicos deberían ser adoptados en el corto plazo?

Personalmente creo que la ciberseguridad debería ser considerada como un bien público de la misma forma que la salud pública y la seguridad. Para llegar a esto es imprescindible que todas las organizaciones impulsen una profunda transformación interna para prepararse ante los nuevos escenarios de riesgo relacionados con el ciberespacio. Para acelerar este proceso es indispensable que el Estado introduzca incentivos que apoyen y reconozca los esfuerzos de las organizaciones en contraposición del modelo clásico de tipo sancionador.

"Los ciberseguros pueden ser un complemento eficaz en la gestión del riesgo ciber para las empresas con cierta exposición a este tipo de amenazas."

4 Informes y análisis sobre ciberseguridad publicados en marzo de 2016

Ciberseguros: la transferencia del ciberriesgo en España (THIBER)

Ciberamenzas 2015/ Tendencias 2016 (CCN-CNI)

Australia's Cyber Security Strategy (Australian Government)

Internet Security Threat report (Symantec)

The UK Cyber Security Strategy 2011-2016. Annual report (UK Cabinet Office)

Buenas practicas para establecer un CSIRT Nacional (OAS)

Review of NASA's information security Program (NASA)

Making Information Security strategic to Business Innovation (RSA)

5 HERRAMIENTAS DEL ANALISTA: SleuthKit y Autopsy

Sleuth Kit® es una colección de herramientas de línea de comandos y una librería de funciones escritas en C que permite analizar imágenes de disco duros y recuperar archivos de ellos. Es ampliamente utilizado en entornos forenses, y es la base de otras muchas otras herramientas de código abierto y forenses comerciales, como Autopsy.

Ilustración 1 Logo de SleuthKit

Autopsy es una interfaz de usuario que hace que sea más fácil de desplegar muchos de los programas de código abierto y plugins utilizados en Sleuth Kit. La interfaz de usuario gráfica muestra los resultados de un análisis forense del volumen de datos subyacente por lo que es más fácil para los investigadores marcar secciones pertinentes de los datos que sean relevantes en la investigación. La herramienta es mantenida en gran medida por Basis Technology Corp. con la ayuda de programadores de toda la comunidad opensource. La compañía vende servicios de soporte y capacitación para el uso del producto.

Ilustración 2 Logo de Autopsy

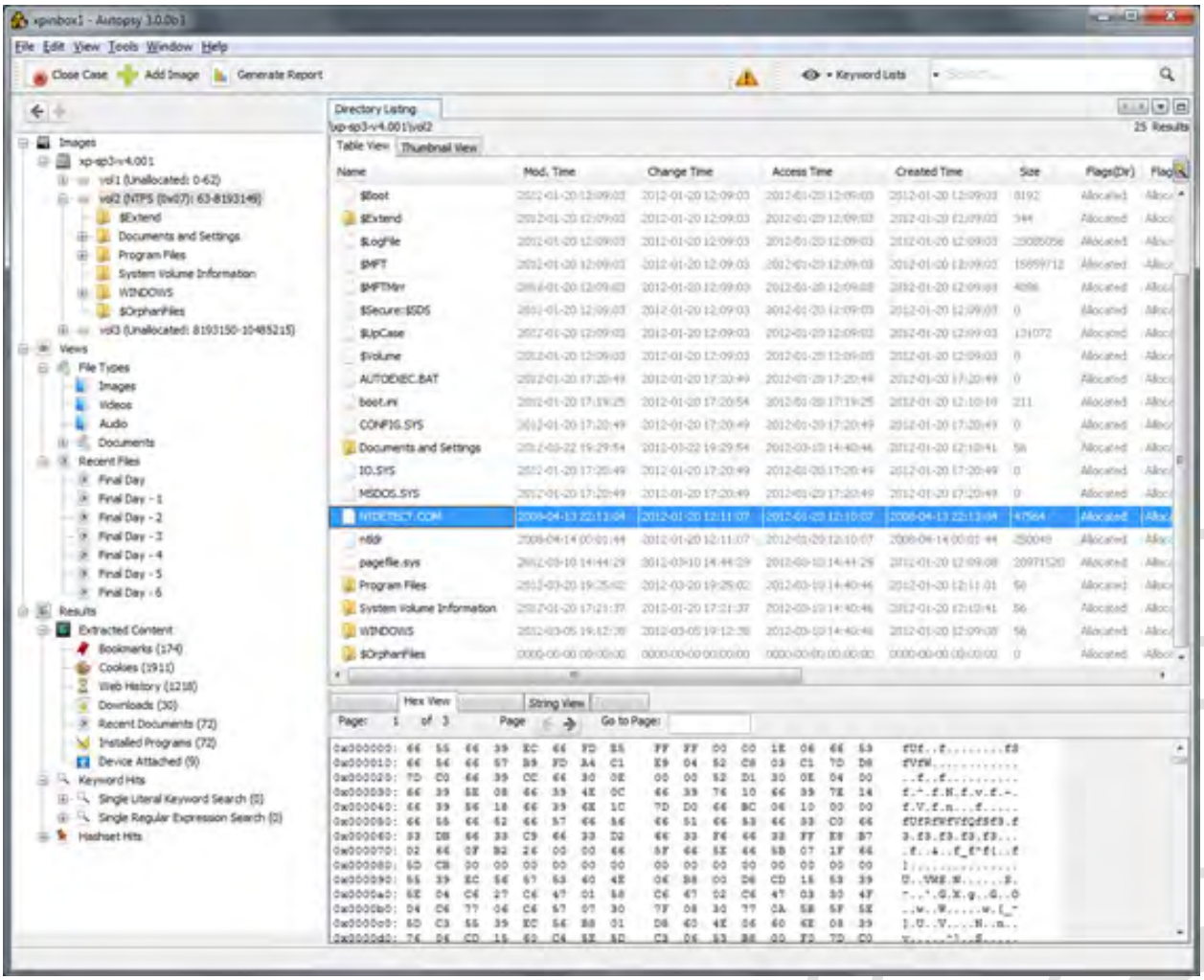
La herramienta está diseñada bajo las siguientes premisas:

- Extensible: el usuario debe ser capaz de añadir nueva funcionalidad mediante la creación de plugins que pueden analizar la totalidad o parte de la fuente de datos determinada.
- Frameworks - La herramienta permitirá implementar algunas prácticas habituales para la ingestión de datos, el análisis y la presentación de informes de cualquier hallazgo, de forma que los desarrolladores puedan seguir los mismos patrones de diseño.
- Facilidad de uso - El navegador de Autopsy ofrece asistentes y herramientas históricas para que sea más fácil para los usuarios repetir sus pasos sin una reconfiguración excesiva.

Adicionalmente permite:

- Realizar análisis temporales (timelines) a través de una interfaz gráfica de eventos.
- Filtrado de hashes: marcando aquellos ficheros identificados como peligrosos e ignorando el resto.
- Búsqueda por palabras: para encontrar archivos que mencionan los términos pertinentes.
- Web Artifacts - Extrayendo el historial de navegación, los marcadores y las cookies de Firefox, Chrome y IE.
- Data Carving: recuperando archivos borrados del espacio no asignado del disco duro usando PhotoRec.
- Multimedia - Extraer EXIF de las imágenes y vídeos.
- Indicadores de compromiso, permitiendo analizar el disco duro en busca de IoCs STIX.

El explorador básico se puede ampliar mediante la adición de módulos que ayudan a escanear los archivos (llamado “ingesta”), navegar por los resultados (“visualización”) o un resumen de los resultados (los denominados “informes”). El conjunto de módulos de código abierto permite una total personalización.



6 Análisis de los Ciberataques del mes de abril de 2016

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

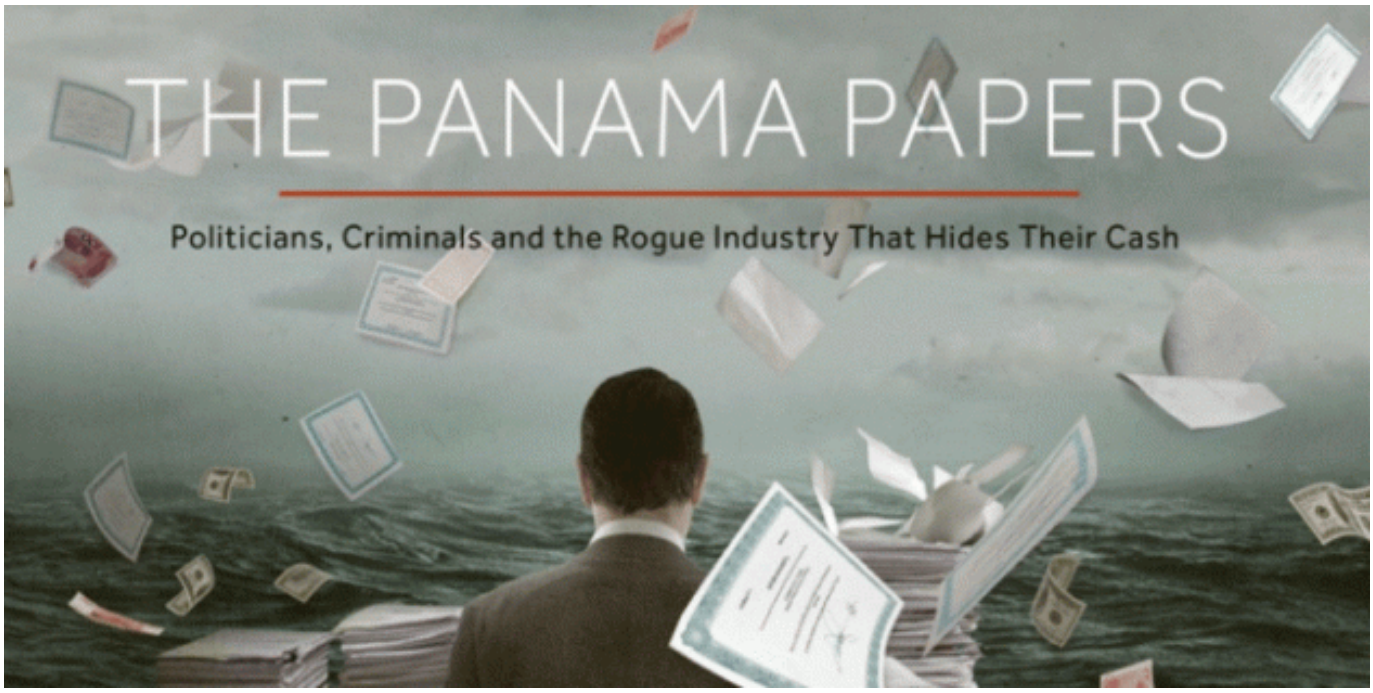
El mes de abril ha tenido un claro actor protagónico: las fugas de datos. Desde diversos bufetes de abogados en Estados Unidos y Panamá, a grandes bases de datos con datos ciudadanos en México y Filipinas.

CIBERCRIMEN

El FBI investiga desde mediados de mes las fugas de datos de dos conocidos bufetes de abogados norteamericanos con especialización en derecho fiscal y corporate: Cravath Swaine & Moore LLP, y Weil Gotshal & Manges LLP. Las redes de comunicaciones de ambas entidades han sido infiltradas por asaltantes externos teniendo acceso a información privilegiada.

En paralelo, *el FBI ha emitido una Notificación Industrial Privada* formal al resto del sector de la abogacía estadounidense advirtiendo de la necesidad de aumentar el nivel de seguridad ante lo que parece ser una campaña de cibercrimen sobre bufetes internacionales de abogados orientada al tráfico de información privilegiada empleada para facilitar proyectos empresariales en tramas de espionaje industrial.

La archiconocida filtración de datos producida a comienzos de mes, al más puro estilo Wikileaks, denominado *"Documentos de Panamá" o Panama Leaks* se ha atribuido a unos criminales que mediante técnicas ofensivas consiguieron acceso a un servidor de correo electrónico del bufete Mossack Fonseca el año pasado.



La fuga de información comprende más de 11 millones de documentos confidenciales de sus clientes, reflejando presuntos mecanismos de evasión fiscal y ocultación de patrimonio en sociedades situadas en paraísos fiscales.

La firma panameña ha contactado a todos sus clientes, afirmando que está investigando cómo se produjo la filtración, y explicando que está tomando "todas las medidas necesarias para evitar que vuelva a ocurrir ".

Casi una semana después de que la firma enviara una alerta a sus clientes anunciando que el servidor de correo electrónico de la empresa fue comprometido, *unos investigadores han identificado que la web principal posee una versión obsoleta de Revolution Slider*, un *plugin* de WordPress, que podría otorgar a un atacante remoto una *shell* en el servidor web, según Feedjit. Éstos han confirmado que su equipo de analistas ha evaluado el historial direcciones IP de Mossack Fonseca y han descubierto que el sitio web de la empresa estaba en la misma red que sus servidores de correo. La nueva página web del bufete de abogados llevaba desplegada algo más de un mes y habría sido «trivialmente fácil» de atacar.

Por otra parte, siempre en el ámbito del cibercrimen, *a comienzos de mes un hacker autodenominado TheNeoBoss* ha conseguido acceder a funciones administrativas en el sitio web porno Skeet Team y ha hecho público en la Deep web estar en posesión de una base de datos que supuestamente contiene direcciones de correo electrónico, contraseñas en texto plano, los nombres y las direcciones físicas y de IP de más de 237.000 usuarios de la página.

También a comienzos de mes *la policía metropolitana de Tokio anunció el descubrimiento de más de 18 millones de credenciales de usuarios de un servidor de la empresa nipona Nicchu Shinsei Corp.* Aproximadamente 1,78 millones de esas credenciales pertenecen a los clientes Yahoo Japón (90 por ciento), Twitter, Facebook, la empresa de comercio electrónico Rakuten y otros sitios web. En respuesta, Yahoo Japón confirmó que ha restablecido las contraseñas de todas las cuentas afectadas. Los investigadores también han descubierto en el servidor una herramienta de hacking utilizado para lanzar ataques de fuerza bruta sobre las cuentas de destino, y también confirmaron que los servidores de la compañía se han utilizado para llevar a cabo transferencias ilegales de dinero.

La policía ha detenido al presidente de la entidad y a un grupo de empleados presuntamente implicados en la trama, ya que se sospecha que permitió a hackers chinos acceder a sus servidores, siendo cómplices de sus ataques.

Varias cepas de un mismo malware fueron detectadas en los sistemas informáticos de la planta de energía nuclear de Gundremmingen unos 100 km de Munich, en Baviera, según han confirmado desde la propia entidad. Tras los primeros análisis, se ha confirmado que el malware puede robar las credenciales de inicio de sesión y permitir que un atacante remoto pueda acceder a los sistemas

La Oficina Federal para la Seguridad de la Información (BSI) alemana ha coordinado la gestión del incidente.

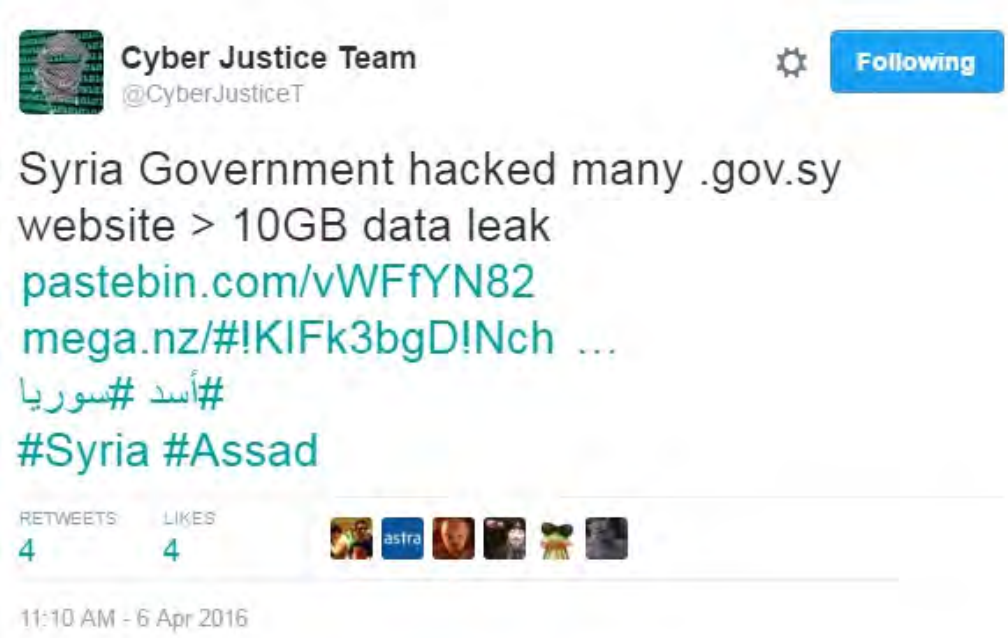
RT
@RT_com
Follow

#German nuclear plants are vulnerable to terrorist attacks – study on.rt.com/783o
10:50 PM - 24 Mar 2016
105 59

A mediados de mes, el grupo de hacking llamado *Cyber Justice Team filtró 10 GB de datos comprimidos* (descomprimidos son más de 43 GB de datos) de varias empresas públicas y privadas de Siria.

El grupo afirmó haber hackeado un servidor Linux que pertenece a la comisión regulatoria de servicios de TI sirio, la Syrian National Agency for Network Services.

El grupo ha subido los archivos en el servicio de alojamiento de archivos MEGA y anunció los datos filtrados en Pastebin, publicando también la contraseña del servidor infiltrado.



Cyber Justice Team
@CyberJusticeT
Following

Syria Government hacked many .gov.sy website > 10GB data leak
pastebin.com/vWFfYN82
mega.nz/#!KIFk3bgD!Nch ...
#سوريا #أسد
#Syria #Assad

RETWEETS 4
LIKES 4

11:10 AM - 6 Apr 2016

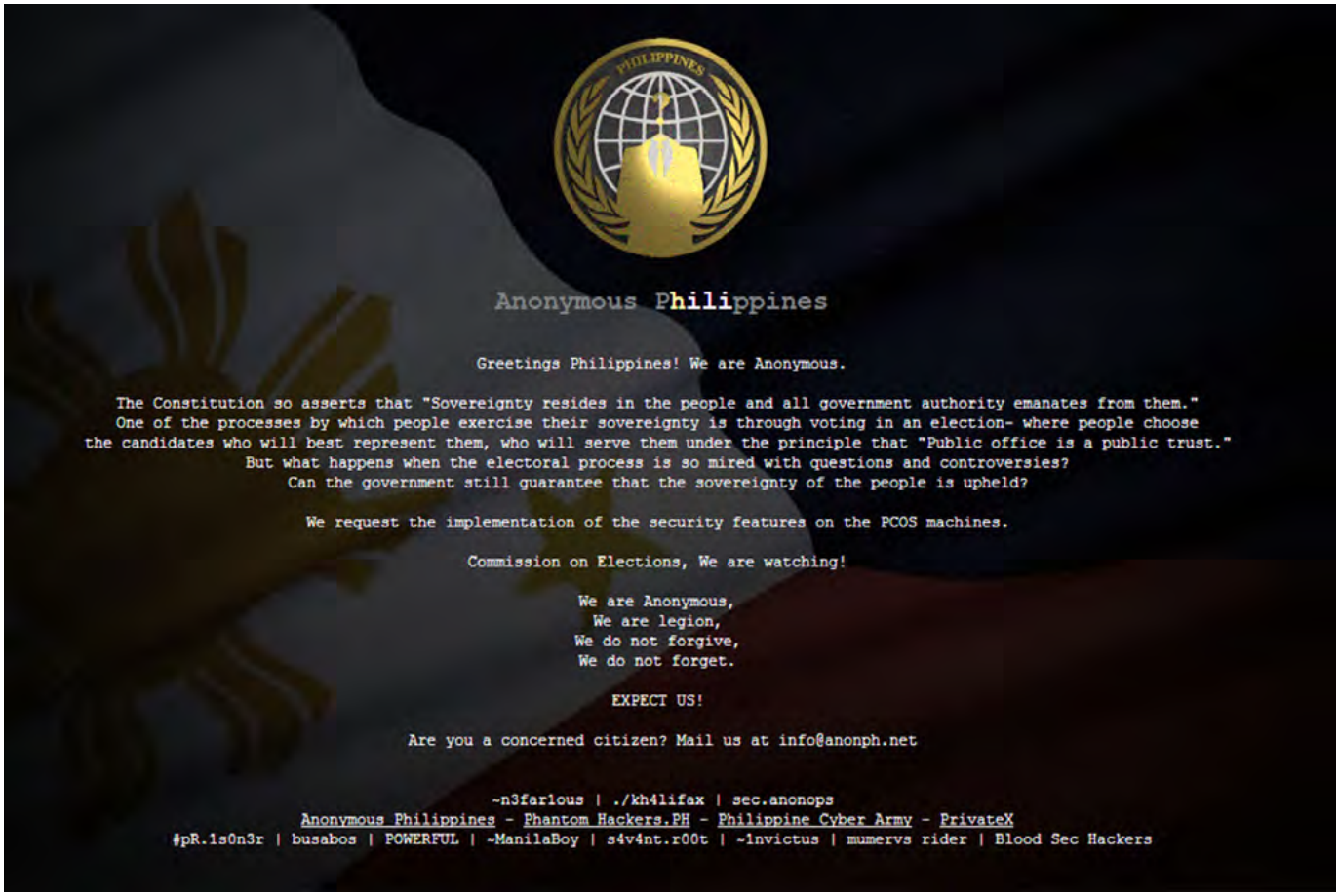
HACKTIVISMO

A comienzos de mes se hacía público un nuevo caso de fuga de información que ha afectado a los sistemas informáticos que soportan los procesos electorales.

En este *caso el afectado ha sido el gobierno filipino.* Su página web encargada del censo electoral fue hackeada durante unas horas mostrando un defacement cuya autoría pertenece a Anonymous filipinas. En dicho comunicado se exhorta al gobierno filipino a mejorar la seguridad de los sistemas PCOS encargados del conteo y validación de los votos a fin de evitar un fraude electoral en las próximas elecciones generales de la república.

Posteriormente se confirmó la filtración de datos afectando a más de 55 millones de ciudadanos (que superaba los 300 GB), incluyendo no sólo datos personales *sino también biométricos (huellas dactilares).*

Este tipo de información sobre votantes es un buen *objetivo de campañas de malware* ya que es muy probable que no todos los partidos políticos con acceso a esta información contarán con sistemas actualizados y con unos estándares mínimos de seguridad.



Posteriormente, el 3 de abril, se hacía pública la *filtración de una base de datos asociada al Sistema Central de Gestión de la Población* (MERNIS, por sus siglas en turco) dependiente del Ministerio de Interior turco que contenía cerca de 90 millones registros con información personal de ciudadanos del país. Dicha base de datos también contenía las del propio presidente del país, Recep Tayyip Erdogan.

El sitio web de MERNIS presenta fallos de programación, siendo vulnerable a diversas modalidades de inyección SQL. El grupo de atacantes parece estar basado en Estados Unidos.

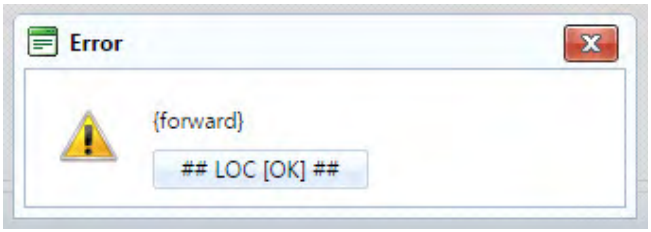
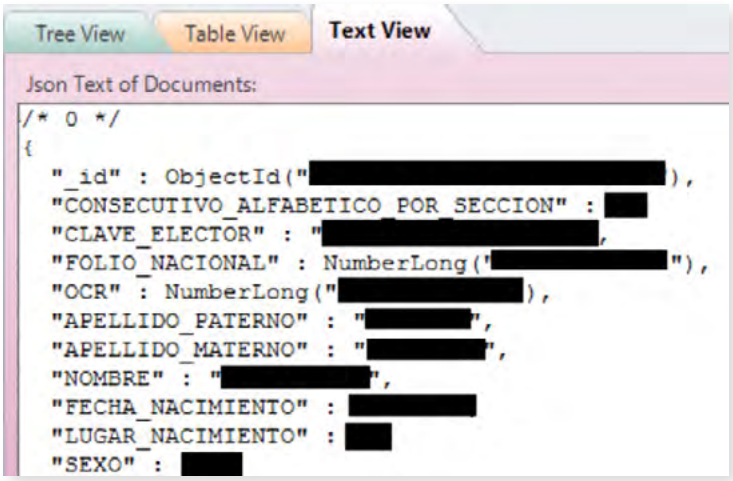


Ilustración Inyección SQL en el portal web de MERNIS

Entre la información filtrada se han identificado campos que muestran el documento de identificación, nombre y apellidos, nombre de los progenitores, ciudad y fecha de nacimiento, sexo, y dirección postal completa (incluyendo ciudad, distrito, calle y puerta).

Ilustración Portal web de MERNIS

Finalmente, a mediados de mes *un investigador de la empresa de seguridad MacKeeper*, Chris Vickery, reveló que la base de datos de la Lista Nominal de Electores —con 93,4 millones de registros que incluyen datos personales como nombre y domicilio de los votantes mexicanos— estaba disponible en un un servidor de internet de Amazon, sin contraseñas ni protección, ante lo cual el Instituto Nacional Electoral interpuso una denuncia penal ante la Fiscalía Especializada para la Atención de Delitos Electorales (Fepade).

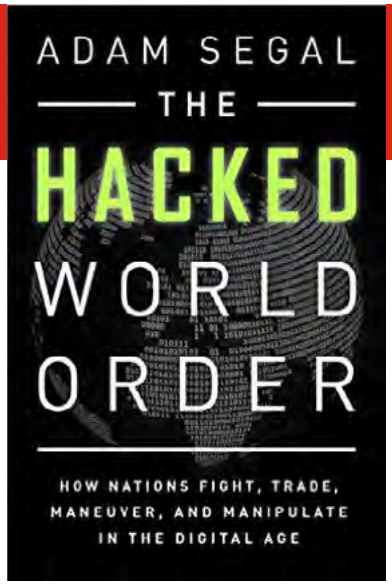


7 Recomendaciones

7.1 Libros y películas

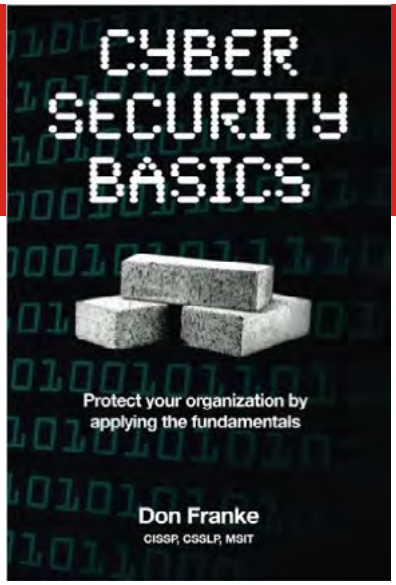
Serie:
PERSON OF INTEREST

Sinopsis: El Sr. Finch es un misterioso millonario, que vive en Nueva York y ha desarrollado un programa informático que predice la identidad de los involucrados en un crimen futuro, ya sea víctima o agresor. Con la ayuda de John Reese un ex-Boina verde y ex-agente de la CIA, ambos intentan detener estos crímenes. Pero, la detective Carter empieza a sospechar quién es el misterioso hombre que logra predecir los asesinatos.



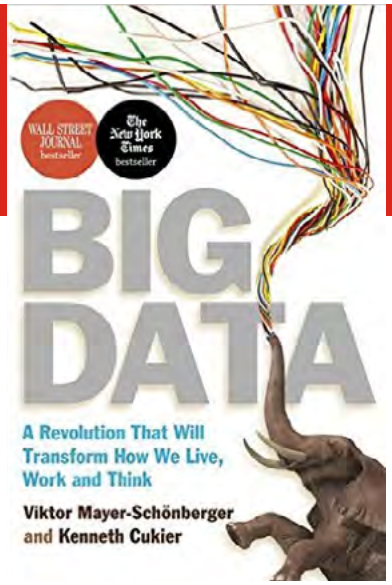
Libro:
HACKED WORLD ORDER

Autor: Adam Seagal
Num. Paginas: 320
Editorial: Public Affairs
Año: 2016
Precio: 15.00 Euros
Sinopsis: Adam Segal analiza como los gobiernos ejercen poder (duro y blando) a traves del ciberespacio. Acciones de guerra, espionaje y sabotaje a traves del ciberespacio empiezan a ser promovidos y patrocinados por cada vez mas gobiernos.



Libro:
CYBER SECURITY BASICS: REMOVING COGNITIVE BARRIERS BY FOCUSING ON THE FUNDAMENTALS

Autor: Don Franke
Num. Paginas: 102
Editorial: CreateSpace
Año: 2016
Precio: 500 Euros (e-book)
Sinopsis: Este libro enumera y analiza de manera didáctica los principales controles que deben ser implementados por una organización para garantizar una correcta seguridad de su infraestructura TIC.



Libro:
BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK AND THINK

Autor: Victor Mayer y Kenneth Cukier
Num. Paginas: 256
Editorial: John Murray
Año: 2013
Precio: 12.00 Euros
Sinopsis: Los autores, dos de los más reputados expertos mundiales en la gestión de datos, analizan la realidad del Big Data y que podemos esperar de su evolución en los próximos 10 años.

Libro:
DATA SMART: USING DATA SCIENCE TO TRANSFORM INFORMATION INTO INSIGHT

Autor: John Foreman
Num. Paginas: 432
Editorial: Wiley
Año: 2013
Precio: 30.00 Euros
Sinopsis: Este libro aborda, desde una perspectiva técnica y tecnológica, la ciencia de los datos. Del mismo modo, analiza las aplicaciones que permiten convertir los datos en conocimiento real.

7.2 Webs recomendadas

https://www.enisa.europa.eu/
Nuevo Sitio web de la Agencia Europa para la seguridad de la información.

http://www.cybersecurity-review.com/
Interesante sitio web promovido por los principales actores en el ámbito de la ciberseguridad para compartir información y conocimiento.

https://www.fbi.gov/about-us/investigate/cyber
Sitio web del FBI dedicado al cibercrimen

https://www.gdt.guardiacivil.es/webgdt/home_alerta.php
Sitio web del Grupo de Delitos telemáticos de la Guardia Civil.

http://www.csoonline.com/
Sitio web que contiene las principales informaciones del mundo de la seguridad informática.

https://eugene.kaspersky.com/
Blog de Eugene Kaspersky, fundador y presidente de la compañía de seguridad global Kaspersky.

7.3 Cuentas de Twitter

@gcolpie

@Sec_Cyber

@derechosdigital

@ticbeat

@computerhoy

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
5 mayo	Madrid	CCI	Encuentro de la Voz de la Industria: Ciberseguridad en el Ciclo de Vida de un Proyecto de Automatización Industrial.	https://www.cci-es.org/web/cci/detalle-evento/-/journal_content/56/10694/220300
7 Mayo	Arganda del Rey	EastMadHack	EastMadHack	http://eastmadhack.org/
8 - 12 mayo	Viena	Crypto Group at IST Austria	Eurocrypt 2016	https://ist.ac.at/eurocrypt2016/
10-13 mayo	Estocolmo	MISTI	13th CISO Europe Summit & Roundtable	http://www.cisoeurope.misti.com/
19- 20 Mayo	Barcelona	APEP	IV Congreso Nacional de Privacidad	http://congreso.apep.es/
18 Mayo	Malaga	Avante	ENCUENTROS E-TIC	http://www.avante.es/evrplus_registration-22/?action=evrplusegister&event_id=15
18- 19 mayo	Washington D.C., United States	INSS	6th Annual Defensive Cyberspace Operations & Intelligence (DCOI)	http://www.dcoi-conference.org/
20-21 mayo	Madrid	X1REDMASSEGURA	X1RedMasSegura 2016	http://www.x1redmassegura.com/
23- 26 mayo	Madrid	MCCD	JORNADAS DE CIBERDEFENSA 2016 DEL MANDO CONJUNTO DE CIBERDEFENSA	https://jornadasciberdefensa2016.es/es
26 mayo	Madrid	ISMS Forum	XVIII Jornada Internacional de Seguridad de la Información	https://www.ismsforum.es/evento/637/xviii-jornada-internacional-de-seguridad-de-la-informacion-de-isms-forum/
26 mayo	Barcelona	Peldaño	Security Forum	http://www.securityforum.es/

www.realinstitutoelcano.org
www.blog.rielcano.org
www.globalpresence.realinstitutoelcano.org

www.thiber.org
twitter.com/thiber_esp
www.linkedin.com/groups/7404269