REAL INSTITUTO elcano ROYAL INSTITUTE

OCTUBRE 2016
Nº 18

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 Ángel Vallejo 09

4 Informes y análisis sobre ciberseguridad publicados en septiembre de 2016... 13

5 Herramientas del analista 14

6 Análisis de los ciberataques del mes de septiembre de 2016 17

7 Recomendaciones

7.1 Libros y películas 24

7.2 Webs recomendadas 26

7.3 Cuentas de Twitter.....26

8 Eventos.....27

1 COMENTARIO CIBERELCANO:
Salvaguardar la soberanía nacional en el ciberespacio

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

Fuente: Diginomica

A pesar de las múltiples escaramuzas y conflictos que acontecen diariamente en el ciberespacio, son muchos los gobiernos que siguen sin comprender el valor estratégico que este tiene para la seguridad nacional. Los ciberataques sobre Estonia que pusieron el país al borde del colapso, el gusano *Stuxnet* que atacó el programa nuclear iraní, las filtraciones de Edward Snowden que revelaron las capacidades de la Agencia Nacional de Seguridad estadounidense o los recientes ataques sufridos por el Partido Demócrata durante la carrera presidencial son solo algunos ejemplos de ciberataques que han causado un gran impacto en la opinión pública mundial, pero su efecto se ha ido desvaneciendo con el paso del tiempo. La realidad es tozuda y mientras las grandes potencias mundiales – Estados Unidos, Rusia, Francia, Reino Unido, China o Israel, entre otras – trabajan en el desarrollo de sus propias cibercapacidades, sobre todo en materia de inteligencia o explotación, buena parte de la Comunidad Internacional observa de manera *impasible la evolución de muchos de estos ciberconflictos.*

Resulta obvio que construir una arquitectura nacional de ciberseguridad fundamentada en capacidades defensivas no es posible; y tampoco lo es hacerlo mediante la adquisición de cibercapacidades a terceros países. Ello es de extrema importancia, puesto que el escándalo Snowden puso de manifiesto que Estados Uni-

dos había estado espiando de forma sistemática y continuada a sus aliados y socios, por lo que muchos países han descubierto la importancia de disponer de capacidades tecnológicas propias que permitan reducir la dependencia externa del país en materia cibernética y minimizar su exposición a la obtención de información por parte de terceros por el simple uso de software o hardware de empresas extranjeras.

En otras palabras, es más necesario que nunca crear, apoyar y potenciar un complejo industrial cibernético que se integre dentro de un sistema nacional de ciberseguridad. El objetivo de este movimiento es muy claro: salvaguardar la soberanía nacional en el ciberespacio. En este sentido ya se pronunció el Ministro de Defensa Pedro Morenés durante el discurso de inauguración de las primeras jornadas del Mando Conjunto de Ciberdefensa celebradas en 2013 cuando resaltó la extrema importancia de disponer de *"…la capacidad industrial para desarrollar nuestros propios mecanismos de seguridad en ciberdefensa".*

A pesar de los grandes escollos que están dificultando la creación de un sistema de ciberseguridad fundamentado en capacidades nacionales autónomas y competitivas, las palabras de Morenés fueron todo un hito porque identificaron una de las raíces del problema.

No cabe duda de que España debe apostar por una industria nacional de ciberseguridad de primer nivel. Talento hay para ello, solo hace falta determinación política.

"España debe apostar por una industria nacional de ciberseguridad de primer nivel. Talento hay para ello, solo hace falta determinación política."

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

Tres ojos sobre Washington: La CIA y sus aliados reflexionan sobre el impacto de la tecnología en el futuro de la inteligencia.

AUTOR: David Barrancos, Analista internacional de THIBER, the cybersecurity Think Tank.

El pasado 20 de septiembre la CIA celebró en Washington D.C. su *3ª Ethos & Profession of Intelligence Conference*, un evento abierto a los profesionales del sector en el que se discutieron las nuevas amenazas y tendencias que afectarán a los servicios de inteligencia en los próximos años. La conferencia reunió por primera vez a tres de los directores de los servicios de espionaje de los Five Eyes, la alianza de inteligencia formada por Estados Unidos, Canadá, Reino Unido, Australia y Nueva Zelanda. Acudieron al evento John O. Brennan, director de la CIA; Alex Younger, jefe del MI6 británico; Nick Warner, director general de la inteligencia australiana; así como su homólogo afgano, Mohammad Masoom Stanekzai.

Durante los diferentes paneles se abordaron los desafíos de algunos de los principales puntos de tensión geopolítica, desde Ucrania hasta el Mar del Sur de China, así como la creciente importancia de la cooperación internacional o la supervisión estatal de los servicios de espionaje. El hilo conductor de todos ellos, sin embargo, fue la tecnología. “La tecnología”, señaló Younger, “supone una amenaza existencial y una oportu-

nidad de oro al mismo tiempo". Como todas las grandes revoluciones, la revolución tecnológica ha actuado como fuerza disruptiva, y los servicios de inteligencia deben saber adaptarse a ella y aprovecharla. "Nuestros servicios", explicó el jefe del MI6, "ya no tendrán que averiguar cosas, sino hacer cosas". "En un mundo en el que cada vez hay menos secretos, la comunidad de inteligencia tendrá que centrarse en anticiparse" avisaba Chris Inglis, antiguo vicedirector de la NSA. Este cambio de rol, concluyeron muchos de los participantes, parece haber llegado para quedarse.

"El futuro de la inteligencia consistirá inevitablemente en formar parte de la revolución tecnológica mientras se desarrollan estrategias para protegerse de ella."

Este esfuerzo por anticiparse ha desembocado en una competición tecnológica entre los servicios de inteligencia de las diferentes potencias. Chris Darby, CEO de In-Q-Tel, el fondo de capital riesgo que invierte en tecnología puntera para la CIA, afirmó que su entidad es ya el tercer mayor inversor en este tipo de tecnología tras Intel Capital y Google Ventures, pero se mostró preocupado ante la posibilidad de que Estados Unidos se esté quedando atrás en algunos campos. "Es cierto que China no tiene la capacidad de innovar que tiene Estados Unidos, pero también somos conscientes de que Escandinavia y Japón fueron los pioneros en el desarrollo del Internet de las cosas, mientras que Estados Unidos llegó después."

Pero si hay una tecnología verdaderamente disruptiva, es, en opinión de los participantes, la tecnología cuántica. "Ahí sí que no queremos ser los segundos", afirmó el ex vicedirector de la NSA.

La tecnología tradicional de cifrado se encuentra amenazada por los nuevos avances en tecnología cuántica. Hasta ahora, los sistemas criptográficos más comunes, como el RSA, basan su proceso de cifra en la multiplicación de dos números primos, una operación simple y rápida de calcular con un ordenador común. Revertir esa operación, sin embargo, es mucho más complejo. La factorización del producto es una tarea que requiere mucho más tiempo desde un punto de vista computacional, incluso para expertos con supercomputadoras.

Un ejemplo bastante clarificador es el resultado de una investigación que trató de factorizar una cifra de 232 dígitos (algoritmo RSA-768). Estos expertos tardaron dos años en finalizar la operación, una duración que en un ordenador estándar de sobremesa podría llegar a los 2000 años. Es precisamente esta prolongación exponencial del tiempo de descrifrado la piedra angular sobre la que se sustenta la criptografía tradicional.

La tecnología cuántica alteraría por completo este proceso de descifrado por fuerza bruta, facilitándolo y haciéndolo mucho más rápido. La computación cuántica no se basa en estados negativos o positivos (binarios) de la información que se transmite, es decir, en 1 o 0, sino que cada bit puede ser al mismo tiempo 1 y 0, un fenómeno similar a la ***paradoja del gato de Schrödinger***. Así un ordenador cuántico podría realizar operaciones matemáticas asumiendo que cada

bit cuántico es a la vez 1 y 0, multiplicando el número de cálculos paralelos por segundo. De este modo, la dificultad y el tiempo de descifrado dejaría de ser exponencial, y el proceso de factorización duraría significativamente menos, incluso en un ordenador personal. Además, una característica destacable de la criptografía cuántica es que permite detectar los intrusos en una comunicación entre dos personas al comparar las bases que han usado ambos (control de integridad).

En definitiva, si esta tecnología no solamente acelera los procesos criptográficos y el criptoanálisis, dejando la seguridad de la información transmitida y almacenada extremadamente vulnerables, sino que además elimina la posibilidad de interceptación invisible de las comunicaciones, es muy comprensible la preocupación de la comunidad de inteligencia. Si una potencia rival llegase a adelantarse en el desarrollo de los ordenadores cuánticos podría acceder a la práctica totalidad de las comunicaciones globales. Igualmente, si esta nueva era criptográfica se convirtiera en la norma a nivel internacional, podría hacer mucho más complicada las labores de espionaje sin ser detectado.

Sin embargo, Jason Matheny, director de *IARPA* –el *DARPA* de la comunidad de inteligencia– llamó a la calma y negó que haya razones para entrar en pánico en el corto plazo. Su organización ya está desarrollando sistemas criptográficos resistentes a la tecnología cuántica, pero también explorando otras posibilidades de esta tecnología en física, medicina o matemáticas. Esta tendencia es conocida por su denominación inglesa como *post-quantum cryptography era.*

Mientras esta tecnología está en desarrollo, los servicios de inteligencia siguen trabajando para resolver algunos de los problemas del cifrado tradicional. El caso de San Bernardino, marcado por la solicitud del FBI a Apple relativa al acceso a los códigos de cifrado del móvil del presunto yihadista, ha marcado un antes y un después en la colaboración público-privada. Para encontrar nuevas vías de colaboración, IARPA está invirtiendo en la denominada criptografía homomórfica, un tipo de cifrado que permite descifrar una entrada de una base de datos sin tener que descifrar la base de datos al completo. Con este tipo de tecnología, cree el director de IARPA, Apple habría sido mucho más proclive a colaborar con la comunidad de inteligencia al reducir su nivel de exposición pública.

Tres años después del escándalo Snowden, el gran elefante en la habitación durante la conferencia, la comunidad de inteligencia estadounidense parece estar más convencida que nunca de que las enormes capacidades de las nuevas tecnologías traen con ellas numerosos desafíos y vulnerabilidades. El futuro de la inteligencia consistirá inevitablemente en formar parte de esta revolución tecnológica mientras se desarrollan estrategias para protegerse de ella.

3 Entrevista a Ángel Vallejo. Socio fundador de MAIO LEGAL. Responsable del área de derecho tecnológico. Director de relaciones institucionales de THIBER, the cybersecurity think tank.

1. ¿Cómo observa el mundo del derecho el desarrollo cibernético?

Creo que el mundo legal comparte con el resto de sectores sociales una cierta sensación de vértigo y, derivado de ella, una preocupación por el acompasamiento de la normativa a la realidad tecnológica.

Mi percepción es que en España conviven todavía dos concepciones enfrentadas del derecho. Por un lado, la de quienes entienden que lo tecnológico no debe afectar al modo en que las normas se crean y aplican y por otro los de quienes pensamos que el desarrollo cibernético es de tal calado que necesariamente cambiará radicalmente las relaciones sociales, que son, precisamente el sustrato del derecho.

2. ¿Hay un efecto real del desarrollo de las TIC en el ejercicio de la abogacía?

El derecho se está viendo afectado (cuando no inmerso) en un cambio que no tiene posibilidad de reversión. Los abogados ya han visto como la gestión de los despachos ha cambiado, los legisladores están sobrepasados por la realidad digital y los jueces (muchos de ellos) parece que no quieren darse cuenta de la modificación que para el derecho supone todo el "nuevo" escenario, desde el Cloud computing al Big Data, pasando por la Inteligencia Artificial.

El ejercicio de las profesiones jurídicas, que es mucho más amplio lógicamente que el de la abogacía, asiste a cambios cualitativos innegables. Hay grandes firmas legales que han establecido partnerships para desarrollar y entrenar herramientas de inteligencia artificial específicamente pensadas para el área jurídica, particularmente el sistema Watson de IBM, cuya evolución cambiará una buena parte de la práctica tradicional del derecho. Sin ir tan lejos, el cloud computing se usa cada vez más en los despachos medianos y pequeños, no solo como base de almacenamiento de datos sino como instrumento para construir y gestionar smart contracts y también para la búsqueda de antecedentes judiciales detallados aplicables al caso concreto. Esto supondrá, además, un cambio en el número y tipo de perfiles de abogados y colaboradores que las firmas profesionales necesitarán incorporar.

3. ¿Considera que el desarrollo tecnológico y la regulación del mismo corren parejos?

En ningún caso. Hay que pensar que el legislador en España (y en la mayoría de países de nuestro entorno) todavía trabaja con protocolos de aprobación de leyes que son indiscutiblemente arcaicos. Esto se refleja necesariamente en una sensación de que las normas van a remolque de la realidad que pretenden regular.

4. En su opinión ¿esto ocurre a nivel nacional o cree que el problema se extiende a otros niveles?

En Europa tenemos una situación peculiar, en la que un amplio grupo de países ha cedido parte de su soberanía normativa en favor de entes supranacionales. En España no se legisla de modo ágil, pero en Europa la situación tampoco es mucho mejor. Dicho eso, parece que la Unión Europea se ha dado cuenta de que la celeridad y el modo en que regule las relaciones cibernéticas pueden marcar de manera definitiva su futuro y el de su estatus en la comunidad internacional.

Incluso con esa idea en mente la aprobación de la Directiva NIS (Network and Information Systems) ha necesitado de más de tres años de trabajo intenso, un plazo que en el actual ritmo de desarrollo tecnológico puede ser una eternidad.

Se están haciendo a nivel europeo cosas muy importantes, y creo que son planteamientos sólidos, pero hay que trabajar para mejorar la agilidad normativa. Dicho eso, no podemos dejar de señalar que la UE ha sido puntera y ha culminado avances esenciales en la mejora de la protección de sus ciudadanos frente a la ciberdelincuencia, entre los que destacan el establecimiento del Centro Europeo de Ciberdelincuencia (IP/13/13), la propuesta de legislación sobre los ataques informáticos (IP/10/1239) y el lanzamiento de una alianza mundial contra los abusos sexuales a menores en línea (IP/12/1308).

Hay una evidente pugna entre la Unión Europea y los Estados Unidos por ver cómo mantienen los segundos su posición hegemónica en el mundo ciber y cómo la primera se esfuerza en no quedarse atrás. A ambos bloques les va mucho en ello.

Lo planteó perfectamente Neelie Kroes, vicepresidenta de la comisión responsable de la Agenda Digital al señalar que *"cuanta más gente dependa de Internet, más gente dependerá de que la red sea segura. Una red segura protege nuestros derechos y libertades y nuestra capacidad de ejercer actividades económicas. Ha llegado el momento de coordinar nuestra acción: el coste de la inacción es mucho más elevado que el de la acción".*

5. ¿Le parece viable la figura de un legislador supranacional dedicado a normativas de áreas ciber?

Se ha avanzado mucho (pero muy despacio) en el área de la cesión de la soberanía normativa. En esto los europeos somos un referente mundial sin ninguna duda. Pero pensar en un cuerpo legislador que no comparta de base los mismos principios culturales y desde luego los mismos intereses políticos resulta hoy día utópico. No lo veo viable en el corto ni el medio plazo. Al final lo que está en liza es más un modelo conceptual de cómo quieren los ciudadanos que sea internet en especial (y el mundo ciber en general) y cómo los gobiernos tratarán de implementar lo necesario para ese fin.

"Se ha avanzado mucho (pero muy despacio) en el área de la cesión de la soberanía normativa. En esto los europeos somos un referente mundial sin ninguna duda."

El ubicuo problema de la atribución en los casos de actuaciones dañosas en la red y la absoluta ausencia de fronteras del mundo digital apuntan a que sería conveniente algún tipo de super-regulador, pero los problemas que plantea ese modelo probablemente sean tantos como los que pudiera solucionar.

6. Por lo que respecta al derecho español ¿considera que contamos con normativa adecuada al mundo digital?

El legislador español es, como la práctica totalidad de los de su entorno, reactivo. Si es difícil para los propios profesionales seguir el ritmo de la cibertecnología y, aún más, alcanzar a entender las consecuencias de índole social y económico de dicho desarrollo, pensemos en un actor que, como decía antes, mantiene protocolos arcaicos para dictar leyes.

Incluso así, considero que en España lo esencial está en estos momentos razonablemente bien tratado. La última modificación del Código Penal ha sido un importantísimo avance legislativo y ha colocado a nuestro país en línea con los más digitalmente activos del mundo en lo que se refiere a la ciberdelincuencia. Otra cosa es que, tras la aprobación de la normativa específica se produzca la necesaria dotación presupuestaria para posibilitar que las fuerzas y cuerpos de seguridad del estado se enfrente de manera eficaz a verdaderos ejércitos de ciberdelincuentes. La modificación de la Ley de Enjuiciamiento Criminal ha supuesto un gran avance, pero sigue habiendo mucho que hacer en cuestión de dotación de medios, si no se quiere ir siempre dos pasos por detrás de los que operan en la ilegalidad.

7. ¿Cree que los ciudadanos se sienten protegidos en su esfera digital por las normas jurídicas?

Esta cuestión es compleja. En primer lugar, creo que la sociedad civil está descuidando sus labores de alerta y autoprotección ante un fenómeno en el que se halla inmersa. No hablo de rechazar el desarrollo digital, pero sí de mantener una posición crítica a la hora de valorar si todo lo que está a nuestra disposición es necesario o simplemente nos viene bien, sin pensar en el resto de implicaciones, como la privacidad y la seguridad.

Nadie puede abogar por una sociedad neoludita, pero tampoco es sensato eliminar todos los filtros sobre la base de que esto supone poner obstáculos al desarrollo. El problema, a mi juicio, es que la comodidad parece haberse instalado como el principio guía de los usuarios digitales, por encima de cualquier otra consideración, y eso no resulta razonable.

Ahí creo que las autoridades y el legislador deben hacer un esfuerzo continuo por formar y concienciar a los ciudadanos porque, por mucha norma que se dicte después, si no se parte de una idea común con la sociedad civil y sus componentes (todos y cada uno de los ciudadanos), el legislador puede verse en un futuro no muy lejano, con unos ciudadanos extremadamente contestatarios frente a casi cualquier regulación.

Los que trabajamos en el mundo del derecho digital nos encontramos con frecuencia ciudadanos (y compañías, aunque éstas últimas cada vez menos) que escuchan con sorpresa que tal cosa o tal otra no está permitida en el mundo digital. Concurre una cierta idea de que el mundo cibernético es ajeno a las normas del mundo "físico" y de que la libertad de actuación en la red está muy cerca de la falta de consecuencias. Esto no es solo una cuestión de conocer o no las leyes, sino de tener interiorizado que cualquier área de las relaciones humanas (en lo económico, en lo contractual…) necesita un cierto orden para funcionar de manera ágil y segura.

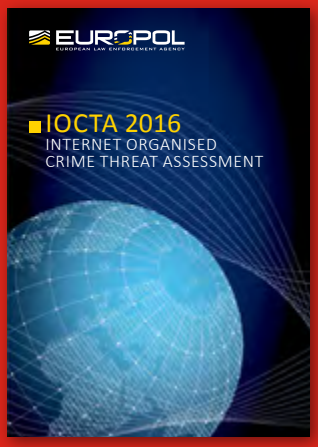
"Concurre una cierta idea de que el mundo cibernético es ajeno a las normas del mundo "físico" y de que la libertad de actuación en la red está muy cerca de la falta de consecuencias."

4 Informes y análisis sobre ciberseguridad publicados en septiembre de 2016

Facing the Cyber risk challenge (Lloyd´s)

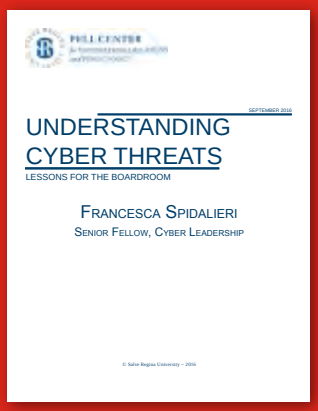
McAffe Labs Threat Report (McAffe)

IOCTA 2016 (Europol)



Cyber Maturity in the Asia-Pacific Region 2016 (ASPI)

Understanding cyber threats (Pell Center)



Guide to Cyber Threat Information Sharing (NIST)

The cost of CryptoMalware (Kaspersky Lab)

Institutions for Cyber Security: International Responses and Data Sharing Initiatives (CISL)

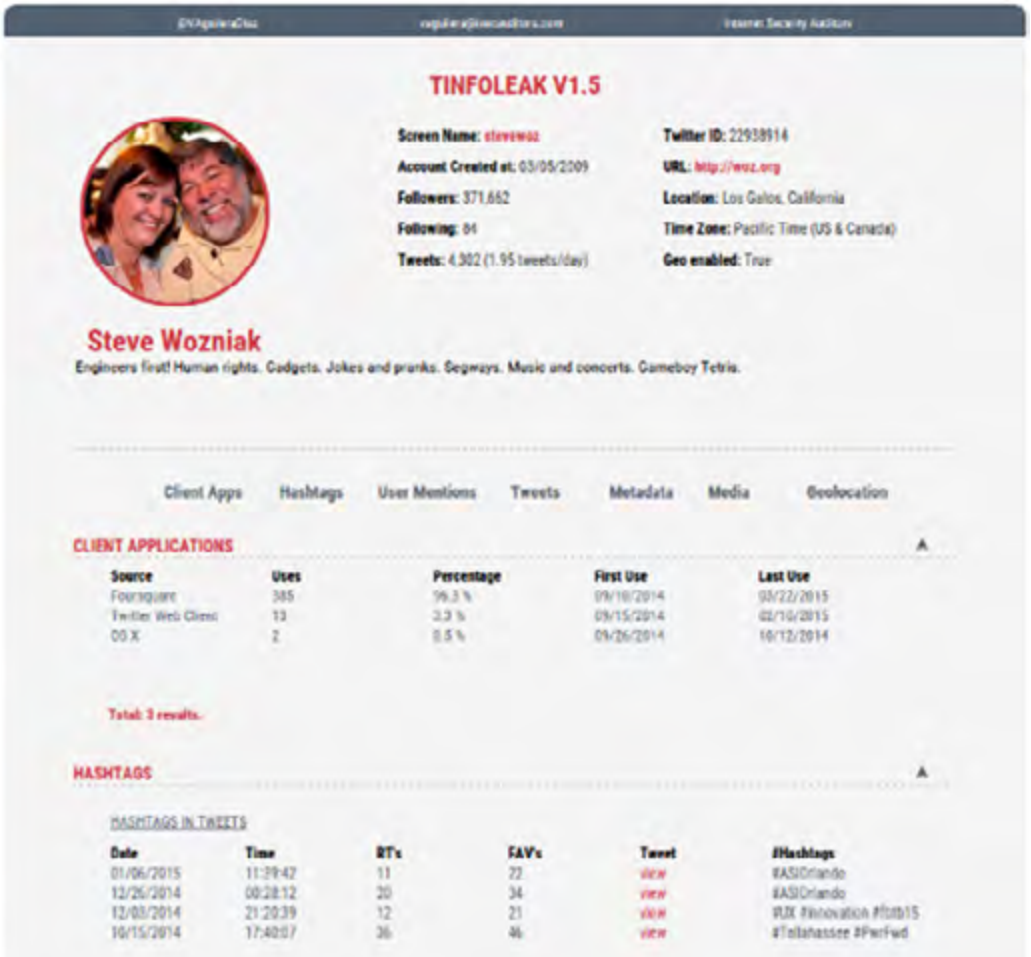
5 HERRAMIENTAS DEL ANALISTA: Tinfoleak

Las redes sociales son una fuente de información sobre nuestra vida profesional y personal. Entre estas redes, Twitter destaca por la actividad de sus usuarios dada la facilidad de uso y su simplicidad. No obstante, en muchas ocasiones, no somos conscientes de todos los datos que facilitamos (directa o indirectamente) y del uso que un tercero puede realizar de la información que publicamos.

Con idea de recopilar información sensible publicada por los usuarios de Twitter, útil para conocer el uso que hacen los usuarios de esta red así como para ser de apoyo en servicios de hacking ético, Vicente Aguilera ha desarrollado la herramienta Tinfoleak que permite automatizar la extracción de información como la siguiente:

Información básica sobre el usuario:

- Imagen del perfil.
- Fecha de creación de la cuenta.
- Número de seguidores.
- Número de amigos (usuarios a los que sigue).
- Número de tweets enviados y promedio de tweets por día.
- ID de Twitter.
- URL extendida.
- Ubicación.



Ejemplo de informe HTML

- Zona horaria.
- Característica de geolocalización.

Aplicaciones cliente:

- Aplicaciones utilizadas por el usuario para publicar tweets.
- Número de tweets publicados por el usuario desde cada una de las aplicaciones.
- Porcentaje de uso de cada aplicación respecto el total de aplicaciones.
- Fecha del primer uso de la aplicación.
- Fecha del último uso de la aplicación.
- Número total de aplicaciones identificadas.

Hashtags:

- Fecha, hora, número de retweets, número de favoritos, y consulta de tweet, de los tweets publicados por el usuario conteniendo hashtags.
- Para cada hashtag utilizado por el usuario, se muestra el periodo de tiempo en el que fue publicado, el número de retweets, el número de favoritos, y el número de veces que fue utilizado.
- Fecha, hora, número de retweets, número de favoritos, y consulta de tweet, de los diez hashtags más utilizados por el usuario.
- Número de hashtags identificados.

Menciones de usuario:

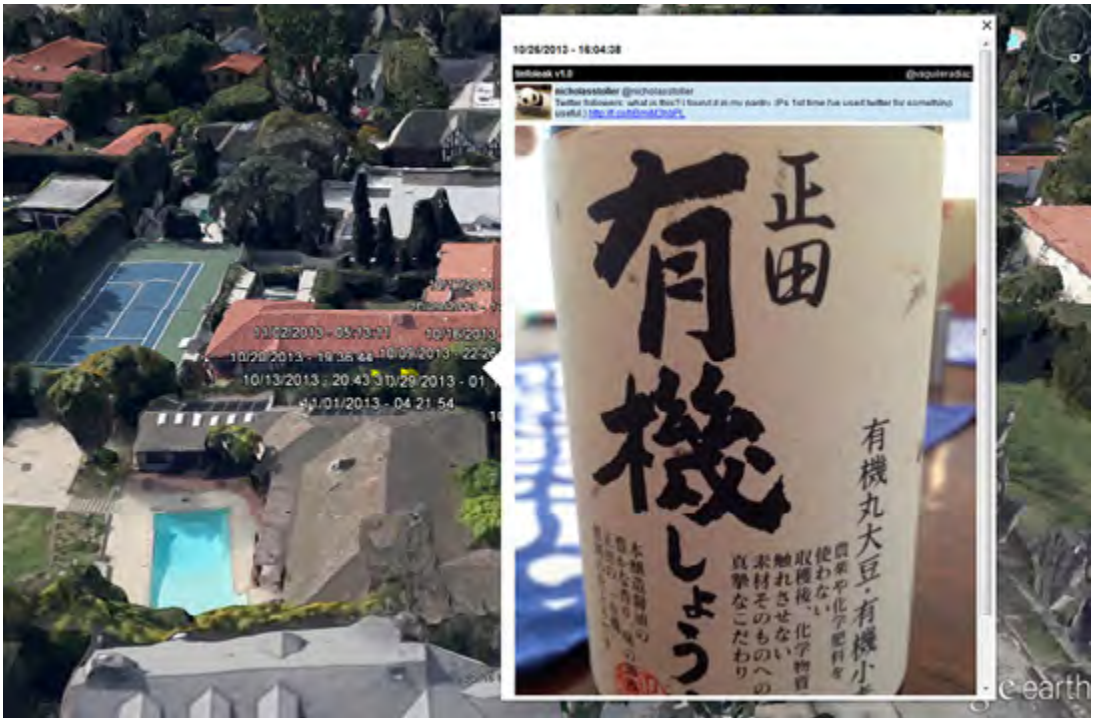
- Fecha, hora, número de retweets, número de favoritos, y consulta de tweet, de los tweets publicados por el usuario conteniendo menciones de usuario.
- Para cada usuario mencionado, se muestra el periodo de tiempo en el que fue mencionado, el número de retweets, el número de favoritos, y el número de veces que fue utilizado.
- Fecha, hora, número de retweets, número de favoritos, y consulta de tweet, de las diez menciones más utilizadas por el usuario.
- Número de menciones identificadas.

GEOLOCATION INFORMATION

TWEETS WITH GEOLOCATION ENABLED

Date	Time	Coordinates	Media	Tweet	Location
03/22/2015	21:01:37	37.249187, -121.875056		view	San Jose
03/22/2015	03:03:44	37.78783834, -122.42157147		view	San Francisco
03/22/2015	02:04:50	37.790352, -122.422409		view	San Francisco
03/21/2015	04:45:07	37.32601085, -122.01519012		view	Cupertino
03/21/2015	02:08:51	37.28769868, -121.94048524		view	Campbell
03/19/2015	21:21:09	39.53029578, -119.81502163		view	Reno
03/19/2015	21:20:30	39.53037679, -119.81515646	Photo	view	Reno
03/19/2015	02:37:51	39.53039323, -119.81517989		view	Reno
03/19/2015	02:36:46	39.53037679, -119.81515646		view	Reno
03/19/2015	02:35:40	39.53037679, -119.81515646		view	Reno
03/18/2015	19:01:21	38.69100342, -121.16216183		view	Folsom
03/18/2015	19:00:39	38.643305, -121.18998		view	Folsom
03/18/2015	19:00:09	38.64270294, -121.18828875		view	Folsom
03/18/2015	04:57:59	37.21581003, -121.96437453		view	Los Gatos
03/18/2015	00:16:23	37.00522, -121.55311		view	Gilroy
03/16/2015	02:47:50	37.331498, -122.033373		view	Cupertino
03/15/2015	17:06:56	37.32305, -121.9981		view	San Jose
03/15/2015	16:08:16	37.61790277, -122.39168644		view	California
03/15/2015	10:40:27	19.43653626, -99.0795422		view	Venustiano Carranza
03/15/2015	10:40:00	19.43655495, -99.07964853		view	Venustiano Carranza
03/14/2015	23:04:44	19.42815371, -99.17914152		view	Miguel Hidalgo
03/14/2015	06:32:10	19.43001034, -99.08041477		view	Venustiano Carranza
03/14/2015	02:18:43	33.43687606, -111.99693561		view	Phoenix
03/14/2015	00:51:21	33.437937, -111.99657083		view	Phoenix
03/14/2015	00:22:11	33.43788776, -111.99694633		view	Phoenix
03/13/2015	20:56:35	51.12985932, -114.01338949		view	Calgary
03/13/2015	20:55:15	51.13011382, -114.01153886		view	Calgary
03/13/2015	18:16:00	51.17576935, -115.5698505		view	Banff
03/12/2015	04:33:24	51.16435559, -115.56181669		view	Banff
03/12/2015	01:19:24	51.13164626, -114.01077032		view	Calgary
03/11/2015	14:45:56	51.47193192, -0.48179508		view	Hillingdon
03/11/2015	14:37:34	51.47266928, -0.48846245		view	Londres
03/11/2015	12:17:35	51.47171, -0.468103		view	Hillingdon
03/11/2015	08:49:21	47.45107236, 8.55906646		view	Kloten
03/10/2015	09:33:27	47.37499, 8.53864		view	Zurich
03/08/2015	13:52:45	47.387385, 8.514282		view	Zurich
03/07/2015	09:29:21	47.40945, 8.545783		view	Zurich

Información de geolocalización de un usuario específico



Geolocalización de una imagen de un tweet

Tweets:

- Se muestran los tweets publicados por el usuario que cumplen el filtro especificado.
- Para cada tweet, se muestra la fecha, hora, y contenido del tweet.
- Número de tweets reportados.

Metadatos:

- Se muestran metadatos asociados a las imágenes.

Imágenes y videos:

- Se muestran las imágenes y videos publicados por el usuario, junto a la fecha y hora de su publicación.
- Número de imágenes y videos publicados por el usuario.

Geolocalización:

- Fecha y hora de la publicación del tweet.
- Coordenadas desde las que se publicó el tweet.
- Información sobre el contenido multimedia (foto o video) contenido en el tweet.
- Consulta en Twitter del tweet geolocalizable.
- Localización asociada a las coordenadas desde las que se publicó el tweet.
- Ruta seguida por el usuario (incluyendo periodo de tiempo en el que permanece en cada ubicación, y número de tweets que envía desde cada una de ellas).
- Localizaciones más visitadas por el usuario, incluyendo periodo de tiempo desde el que publica tweets desde cada localización, número de tweets que envía, días de la semana en los que ha publicado tweets desde cada localización, día de la semana que más publicaciones ha realizado, coordenadas de cada localización y nombre de la ubicación.
- Generación de fichero de salida en formato KML para ser importado desde Google Earth, mostrando los tweets y el contenido multimedia publicado desde cada ubicación.

Generación de informe de resultado en formato HTML

- Permitiendo enlazar con los datos obtenidos y con fuentes externas como Twitter.

6 Análisis de los Ciberataques del mes de septiembre de 2016

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

CIBERCRIMEN

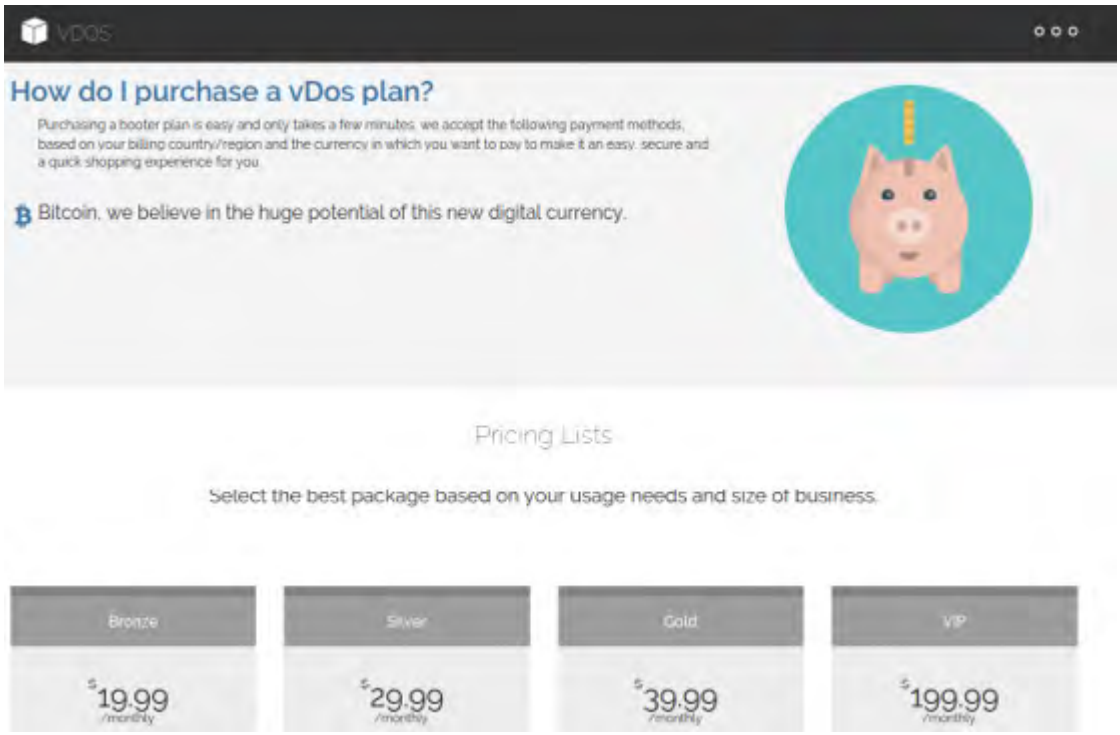
A comienzos de mes, *Dropbox, a través de su blog corporativo*, anunciaba la ejecución de una acción preventiva que conllevaba el restablecimiento de todas las contraseñas de aquellos usuarios cuya fecha de creación de cuenta fuese anterior a 2012.

Diversos analistas de seguridad, posteriormente confirmaron la posibilidad que cerca de 68 millones de credenciales de usuario se hubiesen visto afectadas, extremo que confirmó la propia compañía en un comunicado oficial. Adicionalmente, se ha detectado en un foro de compraventa en la Deep web llamado TheReal Deal, la puesta a la venta de la filtración de datos de la compañía norteamericana, puesta a disposición por un usuario autodenominado peace_of_mind.

El 5 de septiembre, cerca de 800.000 cuentas de usuario del popular sitio web de contenido para adultos *Brazzers han sido expuestos tras una fuga de información de origen desconocido*. Aunque la fuga de datos se originó en un foro separado de la compañía *(http://www.brazzersforum.com/)*, diversos analistas han verificado que un gran volumen de cuentas de usuario coinciden con las de la página principal de Brazzers.

La fuga de datos contiene 790.724 direcciones de correo electrónico únicas, y también incluye los nombres de usuario y contraseñas en texto plano.

También desde comienzos de mes, la página web KrebsOnSecurity del conocido investigador de seguridad Brian Krebs está sufriendo ataques de DDoS de forma "pesada y sostenible". Los ataques se sucedieron desde que el investigador publicó un *artículo sobre la detención de dos atacantes israelíes* de 18 años de edad por su presunta relación con una plataforma comercial para ejecutar DDoS llamado vDOS. Krebs, en su artículo, apuntaba a esas dos personas como los supuestos cerebros detrás de vDOS y puso de manifiesto cómo el servicio de DDoS comercial había recaudado más de 600.000 $ en el último par de años.



Aspecto de la web vDOS para la compra de servicios de DDoS

El *ataque de denegación de servicio distribuido que ha sufrido la mencionada web* ha alcanzado rates de 140 Gbps enviando un único mensaje en cada paquete enviado: 'Godiefaggot', lo que ha forzado a su proveedor de servicios, Akamai, a desconectar la web en varias ocasiones.

Tweet de Krebs aportando datos sobre el DDoS

El pasado *lunes 13 de septiembre, el grupo identificado como Fancy Bears publicaba* información personal y de carácter médica emitidas por diferentes federaciones y organizaciones, afectando a un total de 66 atletas olímpicos de 16 países distintos.

La fuga de datos parece provenir de la Agencia Mundial Antidopaje, conocida como WADA por sus siglas en inglés. El propio organismo ha confirmado el ataque en varios comunicados oficiales atribuyéndolo una autoría rusa.

Web de Fancy Bears asociada al ataque a WADA

Finalmente, *a mediados de mes, se confirmó públicamente que el conocido servicio británico de streaming de música Last.fm* podía haber sufrido una filtración de 43 millones de credenciales de usuario a comienzos de 2012. Esta fuga de información acabó siendo expuesta públicamente a finales de septiembre a través de foros dedicados al intercambio de credenciales de usuarios robadas.

La *información filtrada* contiene nombres de usuario, direcciones de emails, el password hasheado así como diversos datos asociados al perfil de cada usuario.

Last.fm emitió un comunicado en junio de 2012 en el que informaba de una fuga de información de usuarios y, como medida de preventiva, forzó el restablecimiento de las contraseñas de manera inmediata.

CIBERESPIONAJE

En el plano del ciberespionaje, a mediados de mes la *empresa de seguridad FireEye* reveló que dos agencias gubernamentales basadas en Hong Kong han sido objeto de ataques de diversas campañas de ataques orientados a la extracción de información confidencial cuya autoría apunta a China, coincidiendo con el mes previo a las elecciones legislativas locales.

Hasta en tres ocasiones durante el mes de agosto, el grupo de atacantes con sede en China conocido como APT 3, conocido por sus ataques de "spear phishing", en los que se utilizan correos electrónicos con enlaces maliciosos y archivos adjuntos que contienen software malicioso para acceder a las redes informáticas, han centrado sus ataques en objetivos gubernamentales de Hong Kong, bajo una aparente motivación política.

Hasta la fecha no es posible confirmar si APT 3 se encuentra vinculada de alguna forma a alguna organización gubernamental china.

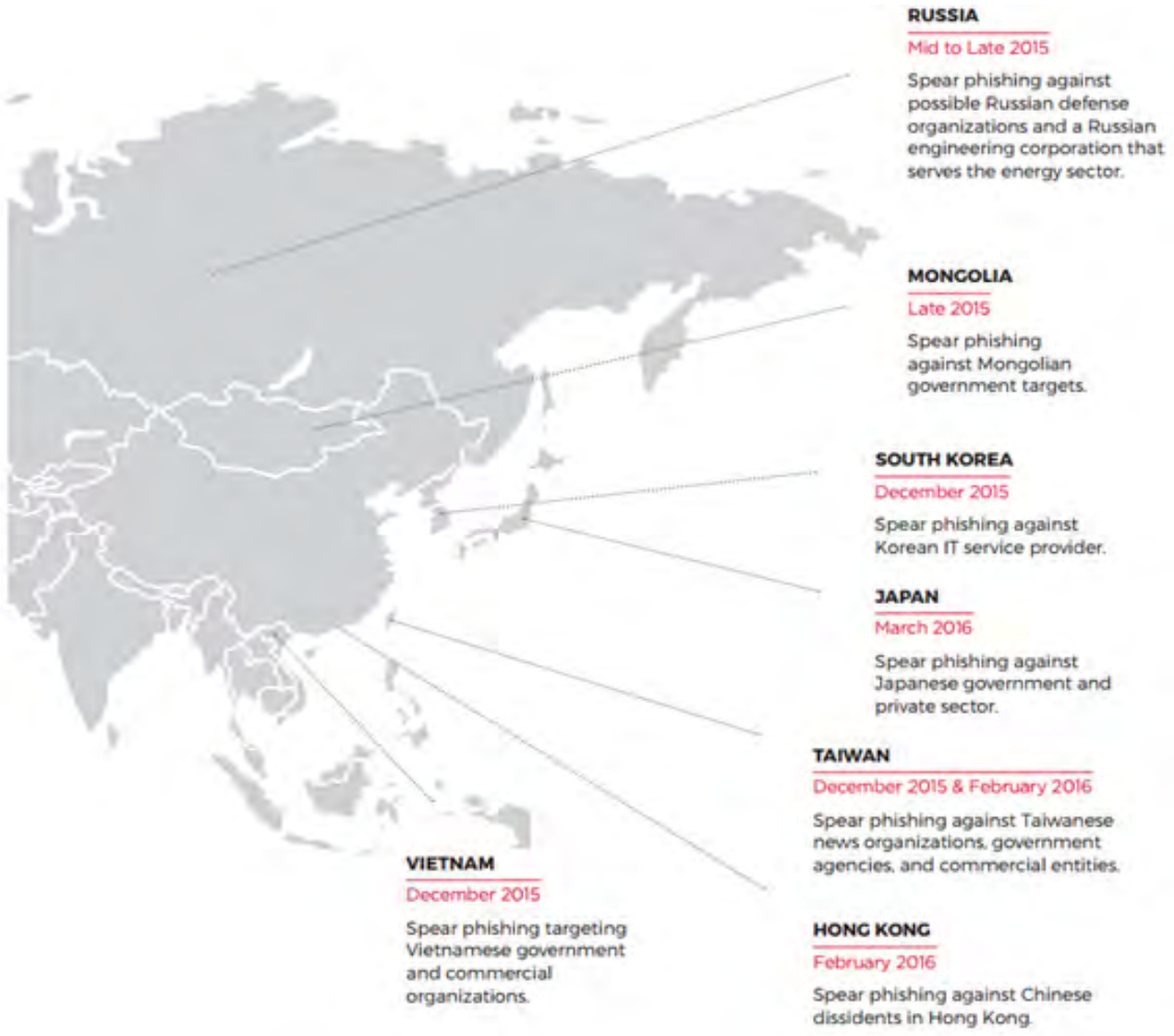


Imagen del informe de FireEye relativo a las acciones cibernéticas ofensivas con posible autoría china

HACKTIVISMO

Desde comienzos del mes de septiembre, *la policía austriaca investiga un ciberataque fallido en el aeropuerto de Viena cuya potencial atribución podría corresponder*, tras un anunció reclamando el ataque, a un grupo nacionalista turco.

El grupo de atacantes autodenominado "Aslan Neferler Tim" o " Equipo de soldados leones", afirman que lanzaron el ataque en respuesta al "racismo" mostrado por las autoridades austriacas del aeropuerto. El grupo se refería a la negativa de los funcionarios a emitir visados de emergencia a un grupo de ciudadanos turcos que habría permitido que saliesen del aeropuerto y pasasen la noche en un hotel de las inmediaciones tras un fallo técnico del vuelo en el que viajaban.

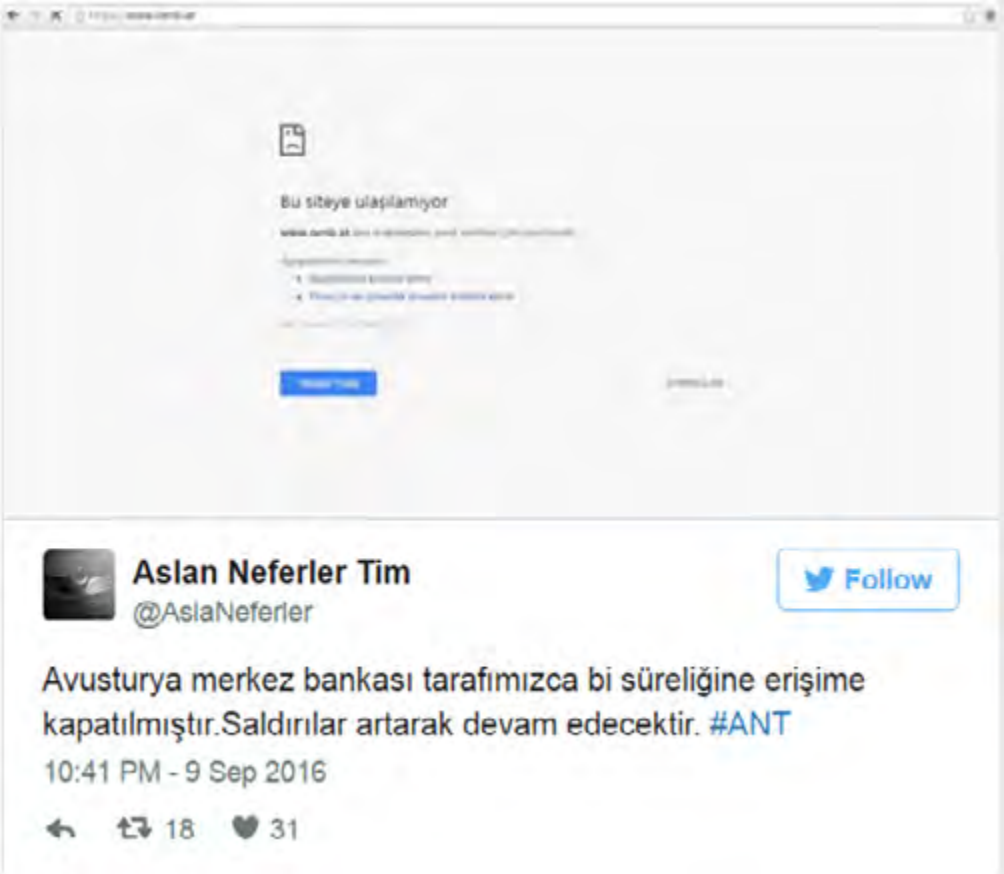
Dichos atacantes se describen como la respuesta a los ataques contra el "Islam y la na-ción (Turquía)." Austria propone que la UE suspenda las negociaciones de adhesión con Turquía.

Tras el ataque sufrido en el aeropuerto, el viernes 9 de septiembre las *autoridades del Austrian National Bank (OeNB) informaron* de un ataque que llevaban sufriendo varias horas.

El OeNV comunicó que el mismo grupo Aslan Neferler Tim estaba reclamando la autoría del ataque de denegación de servicio distribuido (DDoS) que estaba sufriendo el servidor web principal de la entidad financiera.

El grupo turco publicó diversos mensajes en Twitter anunciando que van a continuar los ataques contra organizaciones privadas y públicas austriacas.

Proclama de autoría del grupo turco tras los ataques a objetivos austriacos



Captura de pantalla que muestra la web del OeNB austriaco caído por el DDoS

Por último, un atacante que actúa bajo el pseudónimo MuslimLeets (también conocido como Muj4hida) *llevó a cabo ciberataques dirigidos contra el Consejo Americano del Derechos Humanos (AHRC) y otros 62 sitios web*, afectando a numerosas instituciones y empresas, dirigidas por doctores, abogados y fondos de inversión entre otros. Los sitios web fueron modificados (defacement) con mensajes llamando a la yihad.

El director ejecutivo AHRC Imad Hamad confirmó el ataque a su web, añadiendo que de alguna manera el atacante había tenido acceso a sus servidores. El proveedor del servicio de hosting del AHRC, Novocam, así como diversas autoridades policiales están investigando los ataques.

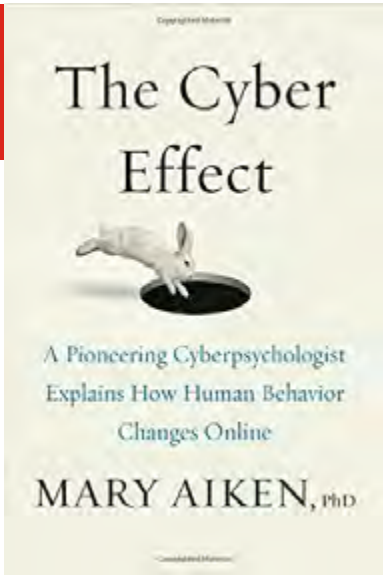
Aspecto que mostraban las webs tras el defacement realizado por MuslimLeets

7 Recomendaciones

7.1 Libros y películas

Película:
WE STEAL SECRETS: LA HISTORIA DE WIKILEAKS

Sinopsis: En la lista de documentales más llamativos de los últimos tiempos, encontramos esta obra sobre una de las fugas de datos más grandes en la historia de del gobierno norteamericano. Este documental nos muestra los principales acontecimientos durante la puesta en marcha del proyecto.

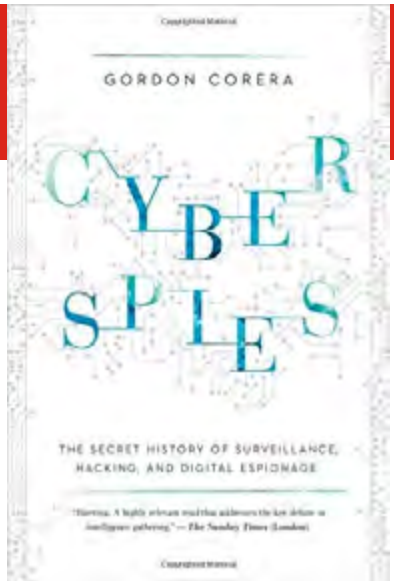


Libro:
THE CYBER EFFECT

Autor: Mary Aiken
Num. Paginas: 400
Editorial: Speigel and Grau
Año: 2016
Precio: 15.00 Euros
Sinopsis: Mary Aiken está considerada como la ciberpsicóloga más prestigiosa del globo. En este libro, Aiken analiza como las nuevas tecnologías están modificando la parte psicológica de las relaciones interpersonales.

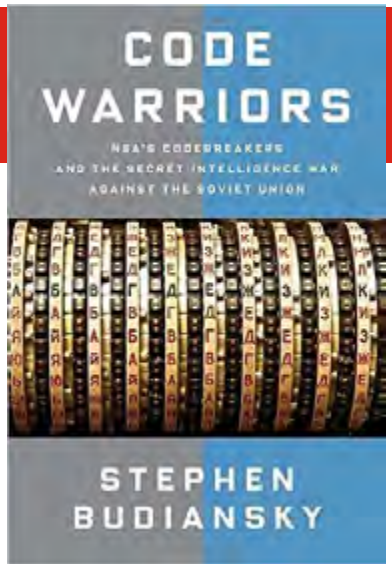
Libro:
SCREENWISE

Autor: Deborah Heitner
Num. Paginas: 240
Editorial: Routledge
Año: 2016
Precio: 16.00 Euros
Sinopsis: Este libro proporciona a los padres y tutores un conjunto de recomendaciones con los cuales podrán gestionar muchos de los retos a los que les someterán sus hijos como nativos digitales.



Libro:
CYBERSPIES

Autor: Gordon Corera
Num. Paginas: 448
Editorial: Pegasus
Año: 2016
Precio: 22.00 Euros
Sinopsis: Este libro relata los principales episodios de ciberespionajes acontecidos a lo largo de la historia protagonizados por las principales potencias mundiales.



Libro:
OUR FINAL INVENTIO

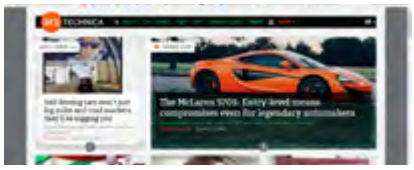
Autor: Stephen Budiansky
Num. Paginas: 416
Editorial: KNOF
Año: 2016
Precio: 18.00 Euros
Sinopsis: Nadie mejor que Budiansky para relatar la obsesión de la NSA por descifrar todas las comunicaciones de los enemigos de los Estados Unidos desde la guerra fría.

7.2 Webs recomendadas

https://www.isao.org/
ISAO es una organización no gubernamental que identifica y analiza aquellos estándares relacionados con la gestión de las ciberamenazas.

https://blogs.akamai.com/
El Blog de Akamai nos acerca análisis sobre las ultimas tendencias en el ámbito de la ciberseguridad.

http://arstechnica.com/
Sitio web que analiza la actualidad de las tecnologías que lideran la transformación digital que vivimos hoy en dia.



https://krebsonsecurity.com/
Sitio web de Brian Krebs , periodista estadounidense especializado en nuevas tecnologías que durante 15 años trabajo en The Washington Post.

https://www.securityforum.org/
ISF es uno de los principales foros a nivel mundial en el ámbito de la ciberseguridad.

http://www.cybersecuritycoalition.be/
Principal iniciativa belga contra el cibercrimen que aglutina actores estatales, sector privado y comunidad academica.

7.3 Cuentas de Twitter

@minsaitbyindra

@gwcchs

@cyberawaregov

@isao_so

@EFOJONC

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
2 Octubre	Indore, India	Hakon	Uncover The Ebola of Underground Black Market – The New Era of Cyber Terrorism	http://www.hakonindia.org/
3 Octubre	Sacramento, CA, EEUU	The Cyber Senate	3rd annual Industrial Control Cyber Security USA	https://www.industrialcontrolsecurityusa.com/
5- 6 Octubre	Londres	Imago Techmedia	Cyber Security Europe	http://www.ipexpoeurope.com/
5- 6 Octubre	Madrid	CCI	VII Congreso Internacional de Ciberseguridad Industrial [4.0],	https://www.cci-es.org/web/cci/detalle-congreso/-/journal_content/56/10694/245896
5 octubre	Verona, Italia	Security Summit Verona	Security Summit Verona 2016	https://www.securitysummit.it/
18-19 Octubre	Dublín	ISC2	ISC2 Security Congress EMEA 2016	http://emeacongress.isc2.org/events/-isc-security-congress-emea-2016/event-summary-8a5426a0038f4b6dbddb288b30fc82b1.aspx
18- 20 Octubre	León	INCIBE	10 ENISE	https://www.incibe.es/enise
18- 20 Octubre	Luemburgo	Hack.LU	Hack.LU	http://www.hack.lu/
19-21 Octubre	San Sebastián	CISIS	9th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2016)	http://www.ehu.eus/ccwintco/cisis2016/
22- 25 Octubre	Berlin	ISF	27th ISF Annual World Congress	https://www.securityforum.org/events/world-congress/isfannualworldcongress2016/
27 - 28 Octubre	Brujas, Belgica	BruCON	BruCON	http://2016.brucon.org/index.php/Main_Page
26 -28 octubre	Bilbao	PESI / ETPIS	S²R European Forum 2016	http://www.s2rforum.es/presentacion/
26 -28 octubre	Buenos Aires	EkoParty	Ekoparty Security Conference	http://www.ekoparty.org/
31 Octubre - 1 Noviembre	Londrés	ISACA	CSX Cybersecurity Nexus Conference Europe 2016	http://www.isaca.org/cyberconference/csxeurope.html

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