NOVIEMBRE 2015 / Nº 8

CIBER elcano

REAL INSTITUTO elcano ROYAL INSTITUTE

Desarrollado por:

THIBER

INFORME MENSUAL DE CIBERSEGURIDAD

REAL INSTITUTO
elcano
ROYAL INSTITUTE

Copyright y derechos:

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank

Índice

1 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
Los casos Google y Safe Harbor. De la batalla ideológica a la disputa comercial estratégica.

AUTORES: Ángel Vallejo, responsable de relaciones institucionales, THIBER. Socio de Maio Legal
Paloma Sánchez-Urdazpal. Maio Legal.

El 13 de mayo del 2014, el Tribunal de Justicia de la Unión Europea (TJUE) colocaba la primera piedra en lo que hoy se conoce como *"derecho al olvido"*. El tribunal resolvía con su sentencia las cuestiones prejudiciales que la Audiencia Nacional de España había planteado a propósito del caso que enfrentó a Mario Costeja y la Agencia Española de Protección de Datos (AEPD) contra Google Spain S.L. y Google Inc. El fallo estableció que los derechos de supresión, bloqueo y cancelación de la Directiva 95/46/CE debían ser respetados por cualquier gestor o proveedor de un buscador, independientemente de lo que hiciese la fuente originaria de los datos personales controvertidos.

En octubre de 2015 el TJUE dictaba sentencia en el caso Maximillian Schrems/Data Protection Commissioner que hacía temblar los cimientos de la transferencia de datos personales entre la Unión Europea (UE) y Estados Unidos. El Tribunal declaraba inválida la Decisión de la Comisión de 26 de julio de 2000 (conocida como Acuerdo Safe Harbor), obligando a la autoridad irlandesa de control *"a examinar la reclamación de Schrems con toda la diligencia exigible y, al término de su investigación, decidir si, en virtud de la Directiva, debe suspenderse la transferencia de los datos de los usuarios europeos de Facebook a Estados Unidos"* al considerar que *"ese país no ofrece un nivel de protección adecuado de los datos personales"*.

La sentencia hizo saltar las alarmas. El acuerdo Safe Harbor sobre transferencia de datos personales de ciudadanos de la UE, plasmado en la citada Decisión de la Comisión se declaraba nulo por completo, provocando una seria tensión con los Estados Unidos. Las reacciones no se hicieron esperar: la Casa Blanca calificó la sentencia como *"profundamente decepcionante"* mientras que Christian Borggreen, director de la Asociación Industrial de Comunicaciones e Informática, que engloba a compañías como Amazon, Google, Facebook o Microsoft, arremetía ante *"The Wall Street Journal"* contra la economía europea, contra las empresas europeas y contra los usuarios europeos. Ningún títere con cabeza.

"El 13 de mayo del 2014, el Tribunal de Justicia de la Unión Europea (TJUE) colocaba la primera piedra en lo que hoy se conoce como "derecho al olvido"

La batalla por la defensa de la protección de datos personales no se está librando sólo en Luxemburgo, a nivel europeo, sino también a nivel nacional. En efecto, el 15 de octubre de 2015 el Tribunal Supremo español dictaba la primera sentencia relativa al derecho al olvido tras el caso Google, concluyendo que la vinculación entre los datos personales de una persona y una información lesiva para su honor e intimidad en una consulta por Internet iba perdiendo su justificación a medida que transcurría el tiempo, en el caso de que las personas concernidas carecieran de interés público o histórico. Añadía también que el derecho a la protección de datos personales justificaba que, a petición de los afectados, los responsables de las hemerotecas digitales adoptaran medidas tecnológicas para impedir que en sus páginas la información obsoleta y gravemente perjudicial pudiera ser indexada por los buscadores de Internet.

La sentencia no afecta únicamente a gigantes como Google, Facebook o Microsoft. Sus consecuencias pueden aplicarse a todas aquellas hemerotecas digitales de medios de comunicación, redes sociales y/o cualquier otra compañía que disponga de ellas y que no esté utilizando los medios necesarios para impedir que la información obsoleta que tengan sobre personas no públicas se indexe por los buscadores de internet.

¿Cuáles pueden ser esas consecuencias? Entre otras, el incremento de reclamaciones contra las compañías que contengan hemerotecas digitales, que contradigan lo establecido por la sentencia del Tribunal Supremo y/o que hayan realizado actuaciones muy similares a las que han sido objeto de la sentencia; la imposición de cuantiosas sanciones a tales compañías; la condena al pago de indemnizaciones a los usuarios afectados por dicho incumplimiento y por los daños y perjuicios causados por ese incumplimiento; y la necesidad de un aumento de presupuesto por parte de las compañías que contengan hemerotecas digitales, a fin de contar con los medios necesarios para evitar que la información obsoleta y perjudicial sea publicada por los buscadores de información.

La batalla no queda ahí: si de momento ya se está aplicando la jurisprudencia sobre *"derecho al olvido"* en los Estados Miembros de la UE y se están anulando acuerdos anteriores sobre transferencia de datos personales, también se está forzando a que la propia UE apure al máximo los últimos meses del año para aprobar el nuevo Reglamento Europeo sobre protección de datos. Una normativa que se espera refuerce aún más la postura de Europa respecto a la protección de datos personales de sus ciudadanos por contraposición a otras políticas más laxas que hacen primar la seguridad del Estado sobre la protección de los derechos a la intimidad y privacidad los usuarios.

Lo anterior, sin embargo, no permite concluir que la UE y sus miembros van en una sola e inequívoca dirección respecto a una cada vez mayor protección de datos personales, y del derecho a la intimidad o al honor. En efecto, estamos asistiendo a una corriente de mayor permisividad o laxitud con respecto a las posibilidades de utilización de ciertos medios y herramientas basados en las TIC, por parte de las fuerzas y cuerpos de seguridad del Estado. Esto ocurre en el Reino Unido y Francia entre otros países.

"se está forzando a que la propia UE apure al máximo los últimos meses del año para aprobar el nuevo Reglamento Europeo sobre protección de datos."

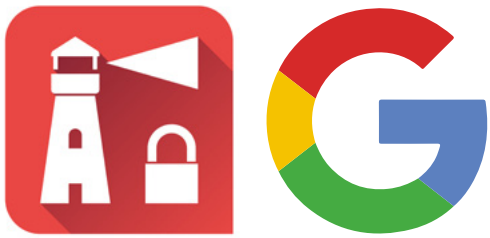
Y ocurre también en España, donde el proyecto de nueva Ley de Enjuiciamiento Criminal (LeCrim) preveía una esencial ampliación de los poderes de intervención de entidades gubernativas y policiales en ámbitos que, como los del derecho a la intimidad y el secreto de las comunicaciones, se han considerado tradicionalmente coto vedado a cualquier intrusión no amparada por una autorización judicial.

La previsión de que la policía y resto de cuerpos y fuerzas de seguridad del Estado pudieran intervenir, por infiltración o monitorización de equipos privados (a través de troyanos y herramientas similares), en la esfera de las comunicaciones personales de los ciudadanos sin autorización judicial provocó el suficiente revuelo en España como para que el texto finalmente aprobado incluyera como imprescindible la intervención de un juez.

Hay que saber que finalmente en España no se ha legislado (de momento, y respecto a esa específica posibilidad de infiltración) en la línea de lo antes expuesto. Pero no puede olvidarse que ya se ha intentado y que se volverá a intentar en el futuro, si se mantiene (como es previsible) la tendencia hacia la ampliación de los estándares de seguridad en detrimento de los de privacidad.

Está por determinar, si es que eso es alguna vez posible, cuánta libertad está dispuesto el ciudadano español (y el europeo) a ceder en aras de una mayor seguridad, pero eso se antoja inaccesible habida cuenta del dinamismo de la tecnología y del uso que de la misma hacen los sectores fuera de la ley de los que el Estado racionalmente debe proteger a sus ciudadanos.

Entretanto, el caso Google (con su derecho al olvido) y el caso Safe Harbor (con las restricciones de transferencia de datos personales UE-USA) parecen ser la punta del iceberg de una tensión real entre dos grandes bloques tecnológicos y comerciales que hasta hace solo un par de años parecía que siempre habrían de ir de la mano en sus desarrollos.



¿Cuánto de los movimientos que hoy estamos viendo en el escenario euro-estadounidense corresponde a dos visiones realmente dispares de lo que debe ser la protección de derechos fundamentales de intimidad y privacidad de los ciudadanos en contraposición a su seguridad?

¿Y cuánto corresponde a estrategias de puro posicionamiento táctico que los dos grandes actores (UE y USA) implementan para intentar alcanzar (el primero) y afianzar (el segundo) una posición de dominio en lo tecnológico y su inevitable derivada comercial?

No cabe duda de que la implementación de la normativa que sobre el Mercado Único Digital se viene preparando en Europa apunta a un posicionamiento conjunto de los países miembros de la UE frente a la hoy indiscutible hegemonía tecnológica (y comercial) de los Estados Unidos, lo que supone una aparente separación de los caminos de ambos grupos.

Pero también es indiscutible que, en la senda del ensanchamiento de las facultades gubernativas de control del ámbito privado permeado por el uso de las TIC en detrimento de las autoridades judiciales, lejos de separarse de los Estados Unidos, la UE (o mejor dicho, sus miembros individualmente) tiende a converger con el amigo americano.

En el escenario descrito está en juego, con mucha mayor intensidad de lo que a priori puede parecer, una buena parte de los principios que hoy se dan por sentados y descontados en Occidente. Es deseable que los grandes árboles permitan ver el bosque, pero no está claro que ese sea el caso en estos tiempos.

2 OPINIÓN CIBERELCANO

Entendiendo STIX a través de Mr Robot

AUTORES: Francisco Jesus Gomez Rodriguez, Global cybersecurity team de ElevenPaths.
Mariano González Espín, Global cybersecurity team de ElevenPaths.

En el entorno actual, con un panorama de amenazas digitales creciente y cada vez más sofisticado, la representación e intercambio de información relativa a eventos de seguridad de la información ha jugado y juega un papel muy importante en la protección de los activos digitales corporativos.

Así pues, un mecanismo que se ha descubierto de especial relevancia para incrementar las capacidades de detección y reacción en el ámbito de la ciberseguridad es el relativo al intercambio ágil de este tipo de información tanto intra como inter organizativo, ya hablemos de entidades públicas o privadas.

En este sentido, dicho intercambio de información se está incrementando con el paso del tiempo. Poco a poco la transparencia se impone frente al oscurantismo predominante y la reticencia corporativa a la hora de compartir datos derivados de ciberataques e incidentes de seguridad, trayendo consigo claros beneficios pero conllevando también algunos "costes" anexos.

Los beneficios son claros: a mayor información, tras procesarla e incardinarla, mejora la toma de decisiones, optimizando las capacidades de reacción y protección. Sin embargo, ser capaces de manejar toda esta información puede convertirse en un auténtico problema.

Cuando la cantidad de información crece de forma masiva aparecen problemas de escalabilidad. Si además la información comienza a ser cada vez más heterogénea, el problema se convierte en un problema global que se debe resolver entre todos los actores involucrados.

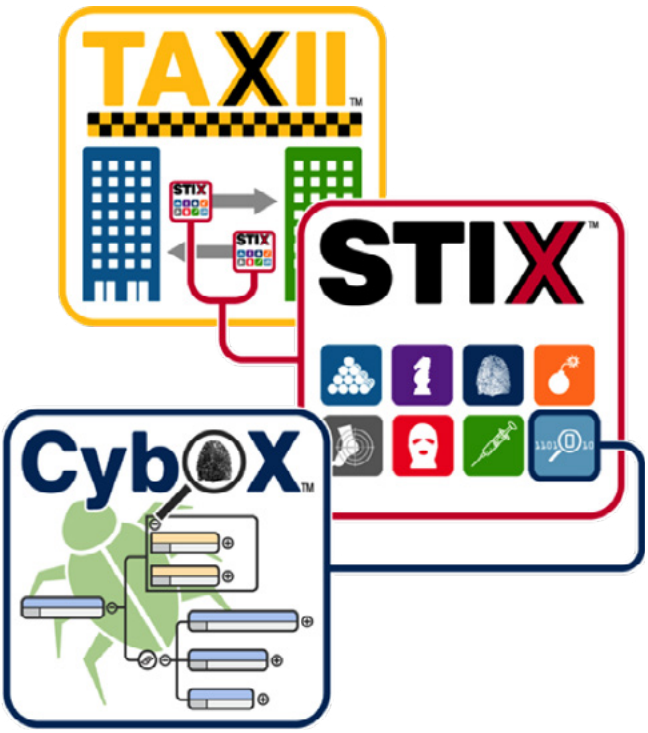
En otros ámbitos, los problemas de comunicación se resuelven compartiendo un único idioma o lenguaje entre los interlocutores. En el mundo de las comunicaciones digitales, para afrontar este hecho, se llevan a cabo procesos de estandarización.

Lo que está claro que la diseminación de la información de ciberinteligencia es una tarea tediosa, sobre todo debido a la falta de normalización de formatos de intercambio y representación de información. No obstante existen diversas iniciativas disjuntas y con diverso grado de madurez y aceptación en el mercado.

"la diseminación de la información de ciberinteligencia es una tarea tediosa, debido a la falta de normalización de formatos de intercambio y de representación de la información"

En siguiente listado muestra algunas de las iniciativas más populares encaminadas a proporcionar mecanismos de intercambio de información que actualmente están siendo desarrollados.

- **TAXII** Trusted Automated eXchange of Indicator Information.
- **CybOX** Cyber Observable eXpression
- **MAEC** Malware Attribute Enumeration and Classification.
- **CAPEC** Common Attack Pattern Enumeration and Classification.
- **IODEF** The Incident Object Description Format.
- **OpenIOC** Open Indicators of Compromise.
- **CIQ** Customer Information Quality.
- **VERIS** Vocabulary for Event Recording and Incident Sharing.



Como en todos los procesos de estandarización existe una guerra abierta por la hegemonía y por convertirse el estándar de factor de la industria. En el caso que compete a este informe, de entre todos los *frameworks* mencionados anteriormente el foco se centra en el definido por *MITRE* por diferentes motivos:

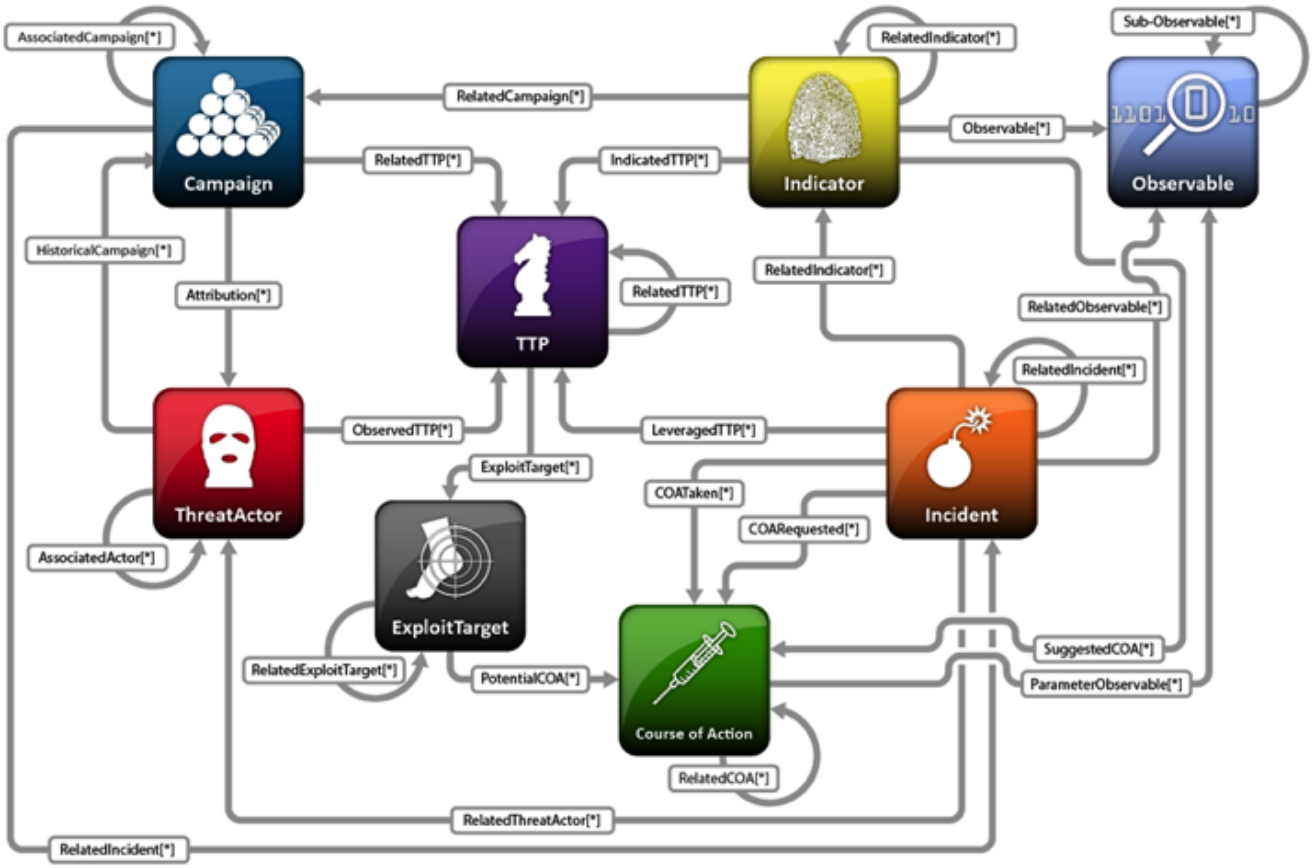
- Como se puede ver en su *web* el estándar se encuentra ya implantado por diferentes actores representativos del mercado, lo que se puede considerar un buen indicador de madurez.
- Permite estandarizar tanto la estructura a través de la cual se representa la información (STIX, CYBOX, MAEC) como la forma en la que las plataformas la intercambian entre sí (TAXII).
- Aporta frameworks específicos para la definición de Indicadores de Compromiso IoCs (CyBOX) y para la representación de malware (MAEC).

A la hora de entender el framework de MITRE lo idóneo es comenzar por asimilar STIX como modelo conceptual de alto nivel para la representación de ciberamenazas, dejando para una segunda iteración la reflexión sobre CybOX, MAEC y TAXII.

STIX propone modelar las amenazas utilizando siete objetos/tipos de datos:

- Actores: como su propio nombre indica, los actores representan las identidades/grupos de identidades que se ven implicadas en una amenaza. El reto para las compañías que quieran implementar STIX se encuentra en poder disponer de un repositorio centralizado y actualizado de actores que permita identificar las actividades realizadas por un determinado colectivo/identidad para poder tanto realizar análisis históricos de su actividad como intentar inferir sus siguientes comportamientos.

- Campañas: el objetivo de las campañas es el de representar de forma unificada diferentes incidentes, TTPs o actores que buscan un objetivo común.
- Incidentes: contiene toda la información relacionada con un incidente de seguridad.
- Observable: los observables son la forma de representación de IoCs (Indicadores de Compromiso) que MITRE ha definido para STIX. Como hemos comentado anteriormente MITRE se basa en CyBOX como lenguaje estructurado para la representación de dichos observables *(https://cyboxproject.github.io/)*
- Indicador: se entiende como un indicador un conjunto de patrones específicos que representan comportamientos de interés dentro de la ciberseguridad.
- ExploitTarget: se utilizan para representar las vulnerabilidades o fallos en la configuración de activos software, hardware o de redes que pueden ser utilizados para atacar los activos de una organización.
- TTP: indican cuál es el procedimiento que se ha utilizado para realizar un ataque o el comportamiento esperado de algún tipo de amenaza.
- Course of Action: son utilizados para representar las acciones tanto de remediación ante un incidente como de prevención antes de que se produzca un ataque.

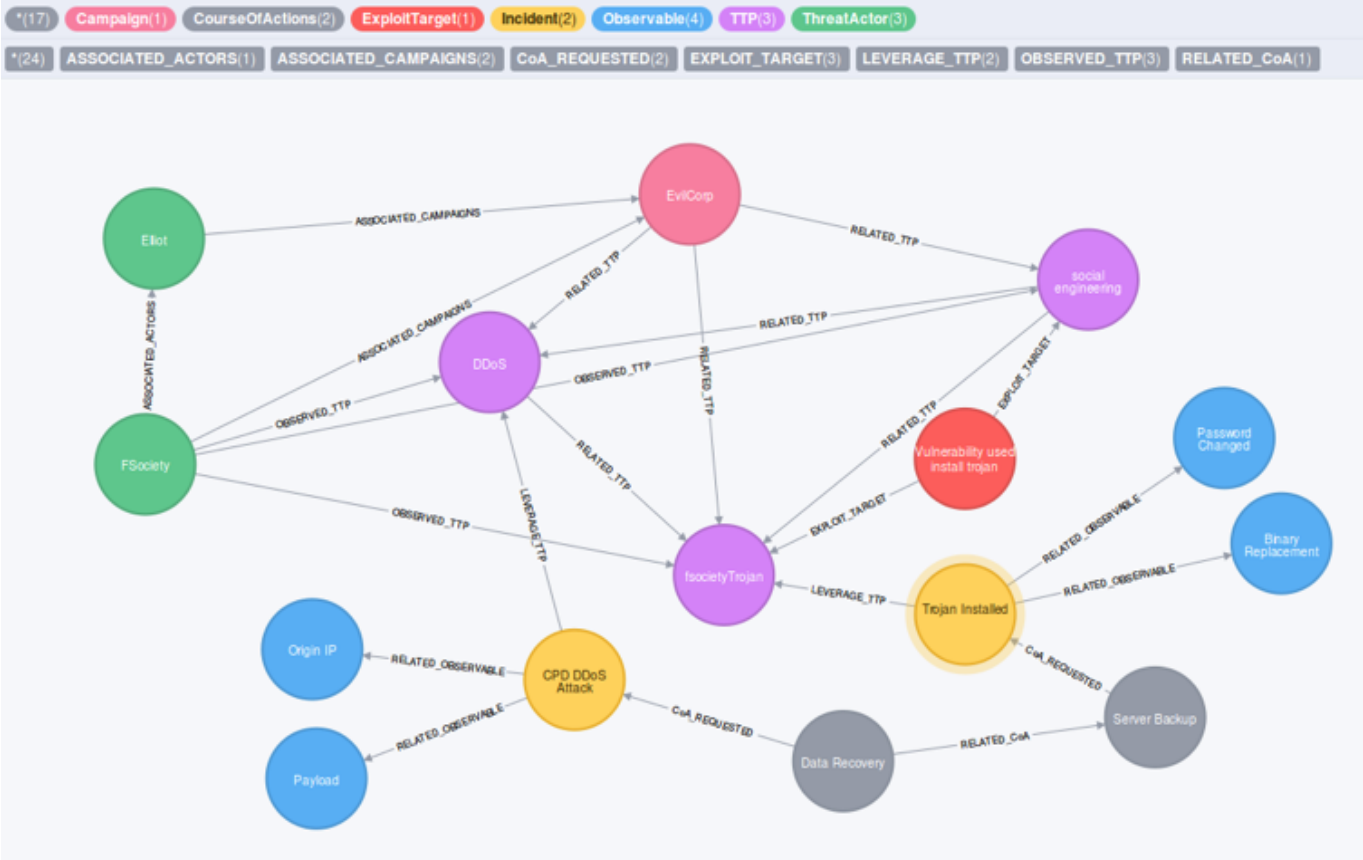


Para entender mejor el modelo de MITRE de una forma didáctica, se ha representado con entidades STIX el ataque que se produce en el capítulo piloto de la conocida serie Mr Robot. Para los que no conozcan Mr Robot es una serie de televisión estadounidense emitida a través de USA Network en la que Elliot, un joven analista de seguridad con problemas psicológicos, inicia su actividad dentro de un grupo hacktivista (FSociety) con el objetivo de acabar con el poder de las multinacionales que controlan las finanzas mundiales.

A modo de resumen, y sin ánimo de desvelar el desarrollo completo del primer capítulo, en el ciberataque que se ha representado, Elliot es llamado para controlar un ataque de dengación de servicio distribuido (DDoS) que FSociety ha lanzado sobre los servidores informáticos de EvilCorp. Una vez que Elliot es capaz de rechazar el ataque, encuentra el fichero origen del ataque (fsociety00.dat) y un fichero readme.txt que le indica que no borre el fichero infectado. Por alguna razón Elliot decide no borrar el fichero y restringe el acceso al mismo para analizarlo con posterioridad. Una vez que Elliot vuelve a casa se encuentra con Mr Robot, un personaje que utiliza ingeniería social para convencerlo de que se una a FSociety y les

ayude a eliminar de forma definitiva los datos de EvilCorp a través de un ataque coordinado entre todos los miembros de FSociety.

El siguiente gráfico (creado sobre la base de datos de grafos Neo4j) muestra la representación modular en STIX del ciberataque anteriormente descrito.



El objetivo perseguido para aquellos que no hayan trabajado con STIX con anterioridad, es que el ejercicio sirva de ayuda para entender a alto nivel la propuesta de tipos de datos de STIX y sea más sencillo hacer una prueba de concepto con alguno de los ataques más frecuentes a los que se enfrentan empresas y usuarios de todo el mundo.

3 Entrevista a Antonio Calderón.
NATO Computer Incident Response Capability (NCIRC) FOC Principal Project Manager

1. Como responsable del Gran Programa de Ciberseguridad de la OTAN, NCIRC FOC, ¿Cómo está afrontando la OTAN los nuevos riesgos en el ciberespacio? ¿Podría trazar los mayores avances en cuanto a su visión global en el ámbito de la Ciberseguridad?

La Ciberdefensa es una tarea fundamental de la OTAN y de su principio de Defensa Colectiva. La OTAN aprobó su primera política en CiberDefensa en Enero del 2008, tras los ataques cibernéticos contra Estonia. Es necesario aclarar que la OTAN es responsable de la protección de sus propias redes de comunicaciones, mientras que las Naciones pertenecientes a la OTAN siguen siendo responsables de la seguridad de sus redes, siendo todas estas compatibles entre si. El "NATO Computer Incident Response Capability (NCIRC)" es responsable de la defensa de las redes de Comunicación e Información de la OTAN.

Del mismo modo, los aliados están muy comprometidos con la mejora del intercambio de información y la asistencia mutua para prevenir, mitigar y recuperase de ataques cibernéticos.

Asimismo, la OTAN está intensificando su cooperación con la industria, y recientemente se han lanzado proyectos tales como el "Cyber Information and Incident Coordination System (CIICS)", una aplicación web que permite a las Naciones autorizadas así como a la industria invitada a compartir información de ciberdefensa dentro de una comunidad de confianza, la "NATO CIICS Federation". Igualmente, los países miembros de la OTAN aprobaron en la última cumbre de Gales en 2014 la "NATO Industry Cyber Partnership (NICP)", que fomenta aun más la colaboración con la industria en estos desafíos comunes en el ciberespacio.

Estos avances se han producido gradualmente pero sin pausa. Desde la cumbre de Praga en 2002, hemos visto forjados multitud de avances en el campo de la Ciberseguridad a nivel político, técnico y operativo. Y ésta probablemente ha sido la clave, que estos avances se han producido en los tres ámbitos, no solamente a nivel técnico. Además, las políticas de ciberdefensa que se han ido incorporando han venido siempre acompañadas de planes de acción específicos y presupuestos acordes a su grado de ambición, autorizados y acordados en consenso. En la actualidad se considera a la ciberseguridad de forma global y aplicada en horizontal en todos los proyectos dentro del ámbito de la Defensa, y ese aspecto es el que mayor trascendencia tendrá de cara al futuro.

"...los aliados están muy comprometidos con la mejora del intercambio de información..."

2. Usted ha sido artífice, en buena medida, y testigo privilegiado de la puesta en marcha de uno de los proyectos más ambiciosos a nivel internacional en el campo de la Ciberseguridad, ¿Cuáles han sido, en su opinión, los mayores retos a los que se ha enfrentado la OTAN en este campo?

Los nuevos retos a abordar en el ciberespacio son cada día más complejos, al ser precisamente un entorno nuevo, en constante redefinición y no siempre comparable con los entornos más clásicos como pueden ser tierra, mar y aire, a los que estamos más habituados. El ciberespacio sigue teniendo un cierto nivel de entelequia difícil de exponer, es por ello que no resulta fácil defender ante un consejo de administración el grado de inversión necesario para gestionar el nivel de ciber-riesgo observado por tu organización, al ser este tipo de riesgos harto difícil de cuantificar, entre otros por la falta de datos históricos. Como consecuencia, uno de los primeros retos que nos encontramos en este ambicioso proyecto "NATO Computer Incident Response Capability (NCIRC)" fue precisamente el de cómo medir el nivel de ciber-seguridad de redes complejas, en nuestro caso englobando las redes OTAN presentes en más de treinta países, incluyendo teatro de operaciones, con multitud de factores de contorno, y traducirlo todo en algo relativamente sencillo que fuese gestionable centralmente día a día. Esencialmente tuvimos que dar respuesta a la siguiente pregunta que se antoja metafísica: "¿cómo se mide un kilo de ciber-seguridad?". Tras varios años de trabajo y desarrollo, en la actualidad se ha alcanzado un grado de madurez muy importante en este campo pionero de la ciber-seguridad medida como un servicio, y no tanto como una capacidad, esto nos ha permitido diseñar unas complejas pero eficientes estructuras de medición del ciber-riesgo.

"¿cómo se mide un kilo de ciber-seguridad?"

Los últimos informes comerciales aseguran que cada día los ataques están más asociados al cibercrimen y a otros aspectos que conllevan el desarrollo de complejas estructuras con una gran inversión. Desde el punto de vista de la ciber-ingeniera el primer reto es estar siempre a la vanguardia tecnológica y ser capaces de mantener esa vanguardia en el tiempo de forma estable, para tratar de estar siempre por delante. Eso requiere de una inversión importante no solo en tecnología y su implementación, pero también e igualmente importante en personal y procesos actualizados de prevención, detección, respuesta, recuperación, operación y mantenimiento. Además, se ha de contar con los mayores expertos internacionales en ciberseguridad y eso requiere de una constante inversión en retención de personal, sobretodo en un campo en el que la demanda supera a la oferta. Otro reto que nos encontramos fue la gestión del cambio. Cuando te enfrentas a la protección de un ecosistema vivo como suelen ser las redes informáticas, y más si abarcan a decenas de países interconectados como en nuestro caso, una vez tienes implantadas ciertas medidas defensivas de ciberseguridad debes de incorporar y mantener un proceso estricto que te permita gestionar la incorporación de cambios necesarios en tus redes sin disminuir el nivel de seguridad implementado originalmente.

3. Hay multitud de países colaborando de forma muy estrecha con la OTAN para llevar a cabo sus cibercapacidades nacionales, ¿Cree que en este campo la coordinación y colaboración es clave para combatir las ciberamenazas crecientes?

Por su grado de inversión y su dilatada experiencia nuestra organización puede proporcionar todos los aspectos que se requieren para lograr una colaboración estrecha en materia de Ciberseguridad, incluyendo aspectos como la formación, la educación, los ejercicios, la gestión y el intercambio de expertos con los países miembros y socios, tanto a nivel político como a nivel técnico y operativo. Pero, además, también requiere de un trabajo conjunto no solo con los países aliados sino también con otras entidades a nivel internacional como la Unión Europea, las Naciones Unidas o el OSCE. En este sentido los diferentes acuerdos y proyectos bilaterales existentes están creciendo considerablemente en este campo, aunque como indicaba el embajador Alexander Vershbow, Secretario General Adjunto de la OTAN, recientemente en su discurso en Madrid, tenemos que mejorar en el intercambio de información e inteligencia, para identificar nuevas vulnerabilidades potenciales conjuntamente.

4. Los grandes países que cuentan con inversiones muy importantes en el campo de la Ciberseguridad, en línea con la OTAN, cuentan con grandes programas desde los cuales se gestionan la implantación de cibercapacidades a nivel nacional, ¿Qué opina de este cambio de paradigma, desde una gestión de micro proyectos hacia la gestión de grandes programas o proyectos? ¿Cuáles son los valores que aporta la gestión de un gran programa en este campo?

Desde su concepción en la OTAN siempre ha habido una orientación a la Gestión de Programas que ha permitido una coordinación adecuada de la Gestión de Proyectos integrantes. En el caso de la Ciberseguridad, es una cuestión bastante interesante y que se puso sobre la mesa hace ya varios años. Aunque la OTAN siempre ha protegido sus sistemas de comunicaciones e información, fue en el año 2002 en la cumbre de Praga cuando la OTAN incluyó por primera vez la CiberDefensa como tal en la agenda política, y desde entonces se ha llevado acabo una apuesta clara por la Gestión de Programas en este campo. Un ejemplo claro fue el proyecto global NCIRC FOC que formó parte de la agenda política tanto en la cumbre de Lisboa en 2010 como en la de

Chicago en el año 2012. Fue la primera vez que un gran proyecto en ciberdefensa llegaba a tratarse al nivel político de una cumbre OTAN. Los países miembros aprobaron la incorporación de nuevas cibercapacidades para la protección centralizada de las redes OTAN y se consideró que la orientación más adecuada era la gestión de un único proyecto con visión global incorporando todo un paquete de capacidades a implementar bajo un mismo marco, dentro del cual fui elegido Gestor principal. Estos marcos de gestión, al fin y al cabo, son una tendencia a nivel internacional por sus grandes ventajas y reducción de riesgos de implementación. Ello te permite considerar y gestionar de forma conjunta todas las interdependencias, riesgos y oportunidades entre los diferentes sistemas y sub-proyectos, y en el campo de la ciberseguridad, es un aspecto clave para llevar a cabo el concepto de protección global de tus redes.

"... la orientación más adecuada era la gestión de un único proyecto con visión global..."

5. En un entorno tan complejo como la OTAN donde el grado de inversión es de miles de millones de euros en tecnología, ¿Cómo se coordinan los grandes programas de ciberseguridad con el resto de proyectos tecnológicos? ¿Cree que se está evolucionando de la forma correcta?

En la actualidad estamos llevando a cabo proyectos específicos para integrar los grandes proyectos tecnológicos con su capa de Ciberseguridad. Al fin y al cabo, la mayor parte de los proyectos tecnológicos requieren, en menor o mayor medida, de una capa de Ciberseguridad. Esto requiere de dos medidas en paralelo que estamos en la actualidad desarrollando. La primera de ellas es la misión de mantener o aumentar las cibercapacidades actuales aplicadas a los diferentes cambios que conllevan los nuevos proyectos aprobados. Para ello, desde la concepción de los sistemas de esos futuros proyectos, durante su etapa inicial de análisis de requisitos, incluimos estos criterios y a lo largo de su ciclo de vida desarrollamos estas capas específicas de ciberseguridad a través de una coordinación común desde la Oficina de Proyectos de Ciberseguridad. La otra medida en paralelo es el desarrollo de nuevas cibercapacidades de defensa demandadas por nuevos sistemas o proyectos. Es por ello que debemos adaptar nuestras defensas continuamente a los nuevos vectores de ataque, amenazas y vulnerabilidades y continuamente estamos elaborando la concepción de nuevas cibercapacidades defensivas a nivel OTAN, no te puedes permitir el lujo de pensar que estas seguro, al contrario.

6. ¿Cuál es, desde su punto de vista y basado en su gran experiencia, el factor clave en el campo de la Ciberseguridad?

En mi opinión, existen multitud de factores críticos a la hora de abordar un gran programa de Ciberseguridad y de dar soporte a su operación, pero sin duda el factor con mayor peso son los recursos humanos. Como apuntaban el Dr. José Ramón Coz y Vicente Pastor en el número 7 de CIBER Elcano cuando analizaron

la problemática sobre la protección de redes, es sorprendente que generalmente en proyectos de ciberseguridad tanto a nivel comercial como gubernamental, este tema de los recursos humanos no sea analizado con la profundidad que requiere, y generalmente se le presta mayor atención y recursos económicos a la tecnología. En el caso de la OTAN me atrevería a decir que contamos con los mayores especialistas a nivel internacional en campos muy específicos relacionados con la Ciberseguridad y que se consideran críticos en este entorno. No obstante, por la propia naturaleza de la organización, se produce una rotación de su personal, principalmente aportaciones nacionales de personal militar de carácter rotatorio, que aunque es también necesaria porque permite que los países se beneficien del conocimiento de los recursos humanos cedidos y que han estado trabajando en este campo dentro de la OTAN durante varios años. Para la OTAN también es beneficioso al nutrirse de expertos ya formados en cada nación con ideas innovativas, aunque todo esto presenta unos retos relacionados con la gestión del conocimiento y las habilidades. Esta rotación se complementa, por supuesto, con una estabilidad en ciertos puestos que se consideran claves. Existen, además, procesos y tecnologías cuya curva de aprendizaje es muy larga en el tiempo y ello requiere de una continuidad. Para solventar esta problemática, se deben aplicar criterios muy sólidos de segregación de funciones y de colaboración con la industria.

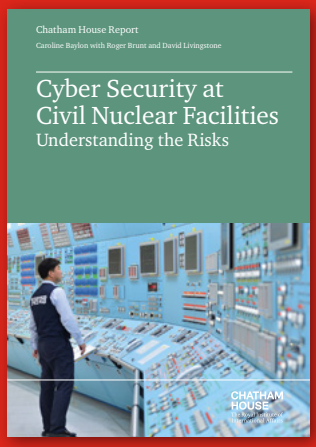
Como conclusión, me gustaría recalcar que los ciberataques podrían llegar a un nivel que amenacen la prosperidad, seguridad y estabilidad de los estados de la zona Euro-Atlántica, y su impacto podría ser tan desastroso como los de un ataque cinético convencional. Por ello, en la cumbre OTAN de Gales en 2014, los lideres de los países miembros decidieron que un ciberataque, según el caso, podría activar el Articulo 5 de Defensa Colectiva.

"... los lideres de los países miembros decidieron que un ciberataque, según el caso, podría activar el Articulo 5 de Defensa Colectiva."

Las opiniones vertidas en esta entrevista son personales y no representan las de la organización a la que pertenece el entrevistado.

4 Informes y análisis sobre ciberseguridad publicados en octubre de 2015

Cyber Security at Civil Nuclear facilitie (Chatham House)



The Tor Dark Net (CIGI)

The Internet Organised Crimen Threat Assessment 2015 (Europol)

European 2015 Cyber Risk Survey Report (MARSH)

Emerging Cyber Threats 2016 (Georgia Institute of Technology)

2015 Data Breach Investigation Report (Verizon)

The implications of Economic cybercrime for policing (Police of London)

Status of privacy and NIS course curricula in EU Members States (ENISA)

5 HERRAMIENTAS DEL ANALISTA:

GRR - Google incident response framework

GRR *(Google Rapid Response framework)* es un framework gratuito opensource para la gestión de incidentes desarrollado por Google y puesto a disposición de la comunidad.

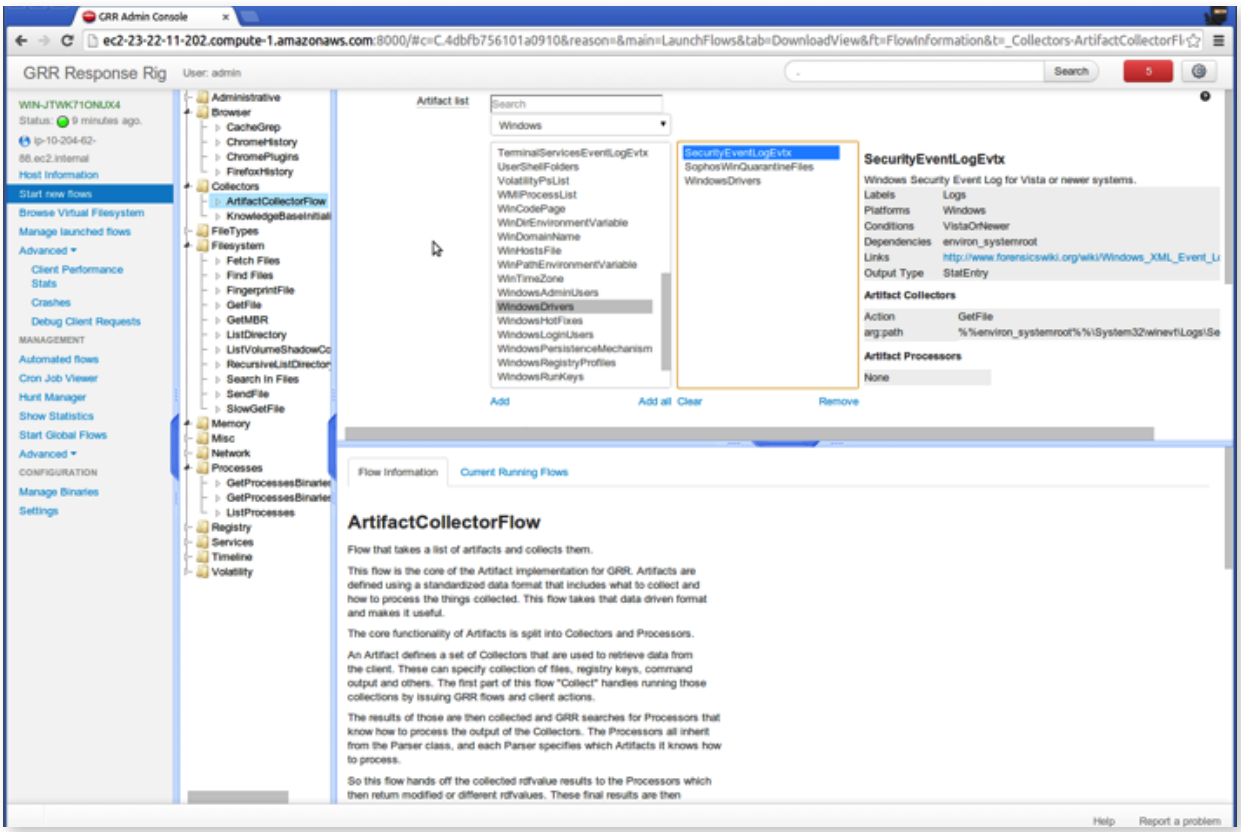
La solución implementa una arquitectura cliente-servidor, mediante la cual un agente (pequeño programa desarrollado en Python) es desplegado en los sistemas que uno podría desear investigar en caso de afrontar un incidente de seguridad. Una vez desplegado, cada sistema se convierte en un cliente GRR y puede empezar a recibir mensajes de los servidores de GRR. Los mensajes remitidos a los agentes permiten ejecutar una acción específica y devolver los resultados asociados. Estas acciones pueden ser simplemente simplemente un código que el agente sabe cómo ejecutar (por ejemplo, la obtención de la lista de archivos en un directorio o la lectura de un buffer de un archivo).

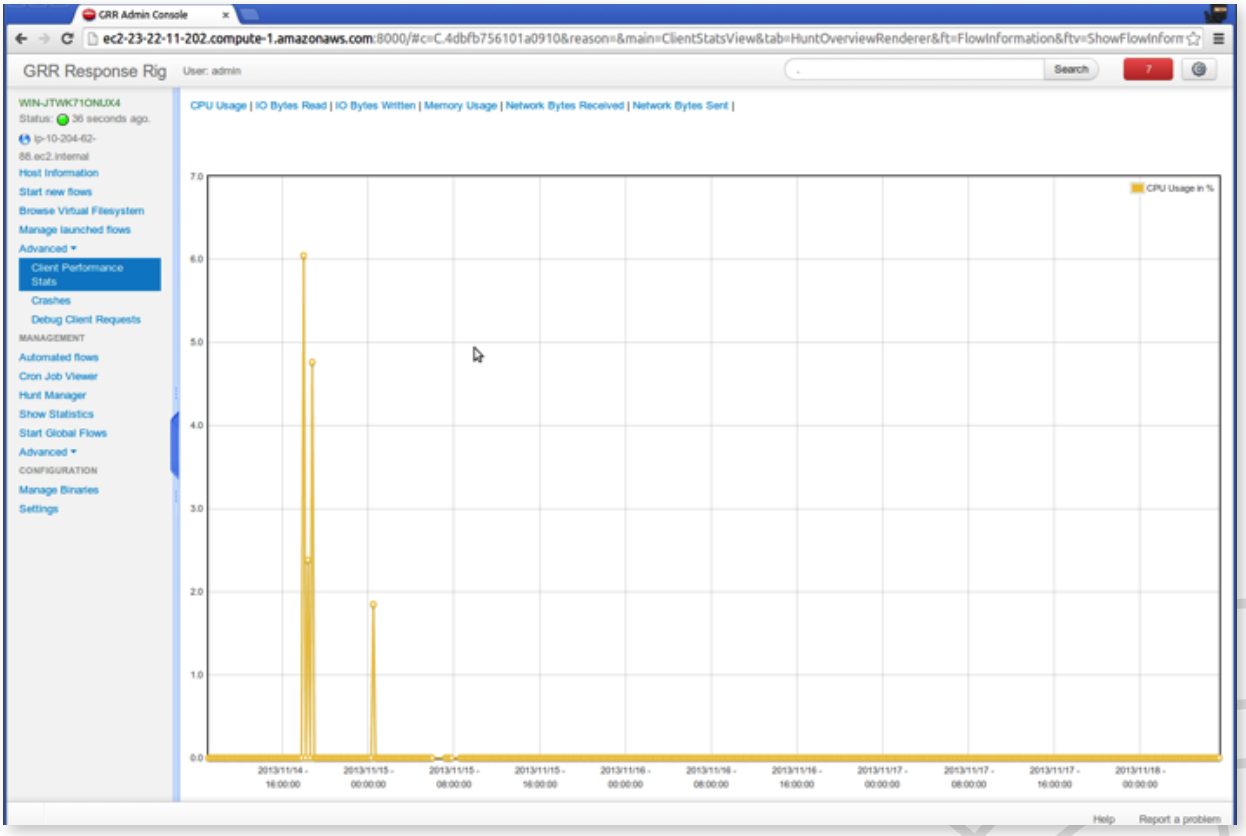
Estas acciones se invocan en el servidor a través de lo que se denominan flujos. Un flujo es una pieza de código ejecutada en el servidor GRR que programa llamadas remotas a los agentes y tiene algo de lógica adicional para decidir qué hacer sobre la base de los resultados obtenidos.

Para ejecutar estos flujos, el usuario puede utilizar la interfaz gráfica que permite al usuario de GRR iniciar flujos en los sistemas clientes y revisar los resultados. También podría haber utilizado la consola para ejecutar las mismas tareas.

Cualquier flujo que se puede ejecutar en una sola máquina también se puede ejecutar como Hunts. Un Hunt es una búsqueda permite ejecutar un flujo completo, o cualquier subconjunto de máquinas del servidor GRR.

Durante una investigación de seguridad postincidente en la que se necesite recuperar rápidamente información que incluyen objetos como tales como ficheros, configuración de servicios, listado de tareas, el estado de parches, cuentas de usuario y mucho más. Estas piezas de información que se conocen como “artefactos forenses”, su ubicación y el formato varían drásticamente entre los diferentes sistemas.


GRR Admin Console
GRR Response Rig
User: admin
Search
Administrative
Browser
CacheGrep
ChromeHistory
ChromePlugins
FirefoxHistory
Collectors
ArtifactCollectorFlow
FileTypes
Filesystem
Fetch Files
Find Files
FingerprintFile
GetFile
GetMBR
ListDirectory
Search In Files
SendFile
SlowGetFile
Memory
Misc
Network
Processes
ListProcesses
Registry
Services
Timeline
Volatility
Artifact list
Windows
SecurityEventLogEvtx
SecurityEventLogEvtx
Windows Security Event Log for Vista or newer systems.
Labels Logs
Platforms Windows
Conditions VistaOrNewer
Dependencies environ_systemroot
Output Type StatEntry
Artifact Collectors
Action GetFile
Artifact Processors
None
Add
Add all
Clear
Remove
Flow Information
Current Running Flows
ArtifactCollectorFlow
Flow that takes a list of artifacts and collects them.
Help
Report a problem


GRR Admin Console
GRR Response Rig
User: admin
Search
CPU Usage | IO Bytes Read | IO Bytes Written | Memory Usage | Network Bytes Received | Network Bytes Sent |
CPU Usage in %
Help
Report a problem

6 Análisis de los Ciberataques del mes de octubre de 2015

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

Octubre ha sido difícil para la banca de inversión y traders, protagonizando diversos incidentes a lo largo del mes. Del mismo modo, como ya sucediera en meses anteriores, hemos asistido a fugas de información de cierto calado.

CIBERCRIMEN

A comienzos de mes, *unos atacantes irrumpieron en un servidor de T-Mobile* llevándose nombres, números de licencias de conducir, y otra información personal perteneciente a más de 15 millones de consumidores estadounidenses.

La infracción fue el resultado de un ataque contra una base de datos mantenida por el servicio de informes de crédito Experian, que fue contratada para procesar solicitudes de crédito para los clientes de T-Mobile, *según comunicó el CEO de T-Mobile John Legere.* La investigación asociada mostró que el ciberataque ha afectado las personas que solicitaron el servicio de T-Mobile desde el 1 de septiembre de 2013 hasta el 16 de septiembre de este año. Este evento representa la tercera fuga de datos conocida que afecta a Experian desde marzo de 2013.

El trader online *Scottrade ha sufrido un robo de información* que ha supuesto la exposición de los datos personales de 4,6 millones de clientes. Empleados de Scottrade han filtrado que el ataque ocurrió a finales de 2013 o principios de 2014 filtrándose números de seguridad social, direcciones de correo electrónico y "otra información confidencial".

Tal y como ya se analizó en el anterior número de CIBERelcano, el vector de ataque fue similar al empleado en el incidente de Patreon. Los propios empleados han comunicado a los medios que no se han visto comprometidas las contraseñas de los clientes así como tampoco se ha detectado actividad fraudulenta tras el incidente.

Como ya adelantábamos, otros dos players del Mercado bursátil, el broker de divisas FXCM y E-Trade, reportaron haber sido víctimas de sendos robos de información notificando que lo atacantes han podido robar fondos de *algunas cuentas en el caso de FXCM* y *algunos datos personales en el segundo.*

Por otra parte, y ya en territorio nacional, *Malwarebytes detectó una nueva campaña de publicidad maliciosa* en seis de las webs de descarga de torrents más grandes de España, exponiendo alrededor de 84.200.000 de usuarios a una cepa específica del ransomware CryptoWall.

Una empresa de publicidad online no suele ser el objetivo habitual de ciberataques pero esto resultó en una situación bastante delicada debido al amplio rate de afección a través de malvertising.

CIBERESPIONAJE

Un estudio publicado a mediados de mes denunciaba que entre marzo y agosto de 2014, 58 ordenadores y dos servidores del metro de *Seúl* fueron hackeados. Los ataques no fueron detectados hasta el mes de julio, cuatro meses después de haber comenzado. Tras haber sido reportados estos incidentes, primero al ayuntamiento de la ciudad, y después a la Inteligencia surcoreana, sospechando que los autores del ataque podría tener vínculos con *Corea del Norte.*

La investigación ha concluido y no se ha podido señalar a un culpable, aunque las pesquisas apunten hacia su vecino del norte, según ha informado la cadena estadounidense, CNN'. A pesar de no haber podido confirmar las sospechas, el ministro de *Defensa* surcoreano mantiene que Pyonyang está empleando su famoso Bureau 121 (ciberejército) para desastibilizar su nación.

Pyongyang por su parte niega estar detrás de los ataques informáticos del año pasado contra el Metro de Seúl.

Sin embargo, los servicios de Inteligencia de Corea del Sur afirman que las tácticas utilizadas en el ciberataque contra el Metro de la capital coinciden con las utilizadas en 2013 en los ataques contra empresas financieras y de comunicación del país.

Por otra parte, los investigadores de Dell *SecureWorks han publicado un análisis de un equipo llamado Threat Group 2889*, que está utilizando al menos 25 perfiles de LinkedIn falsos pero desarrollados minuciosamente para atraer a posibles objetivos en el sector telco, agencias gubernamentales y contratistas de defensa.

A comienzos de mes, *investigadores de Check Point* dieron a conocer los detalles de una campaña dirigida al sector público israelí, usando un exploit kit de Microsoft Word para distribuir una versión modificada del malware Zeus.

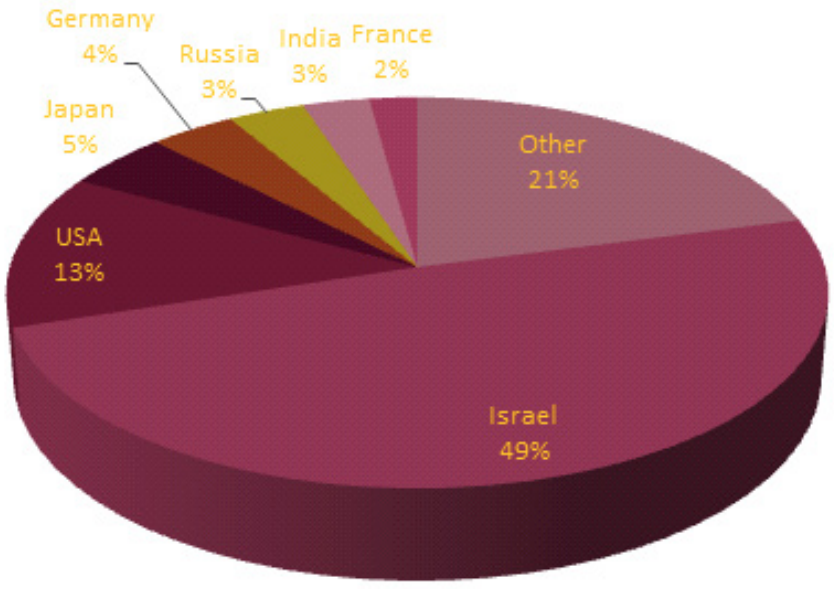


Ilustración: Distribución de las víctimas de la campaña descubierta por CheckPoint

El 20 de octubre, *un estudiante de secundaria afirmó* haberse infiltrado la cuenta de correo electrónico personal del director de la CIA John Brennan. La CIA y las agencias policiales estadounidenses están investigando el caso. El adolescente comunicó al New York Post que había accedido a documentos relacionados con el entorno laboral del director de la CIA, incluyendo una de 47 páginas del Brennan para el despacho de alto secreto seguridad.

El joven hacker explicó que usó la "ingeniería social" para convencer a los empleados de Verizon para que le facilitasen la información personal del director de la CIA y la explotación posterior del servicio de restablecimiento de

contraseña de la AOL.

Posteriormente el volcado de los emails apareció publicado en Wikileaks.

Otros acontecimientos notables del mes en el plano del activismo en la red incluyeron los ataques distribuidos de denegación de servicio (DDoS) contra los dos principales aeropuertos japoneses (Narita y Chubu), dejando gran parte de la infraestructura paralizada por más de 8 horas. Esta acción *fue ejecutada por Anonymous bajo la operación #OpKilling Bay* (la campaña en contra de la masacre de delfines) y en contra de varios sitios web del Gobierno belga ejecutados por la rama local del mismo colectivo.

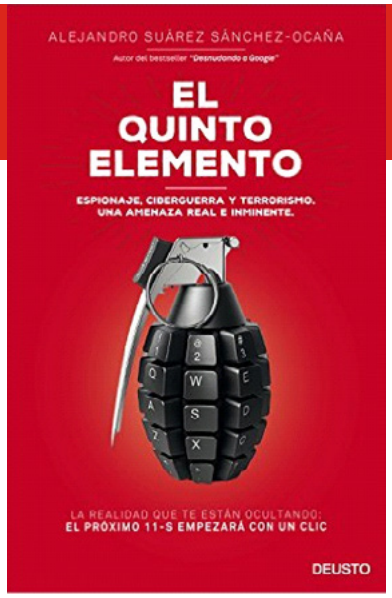
La campaña #OpKillingBay comenzó en noviembre de 2013, con un día de acción antes de volver a encender de nuevo con ferocidad fresca en las últimas semanas.

7 Recomendaciones

7.1 Libros y películas

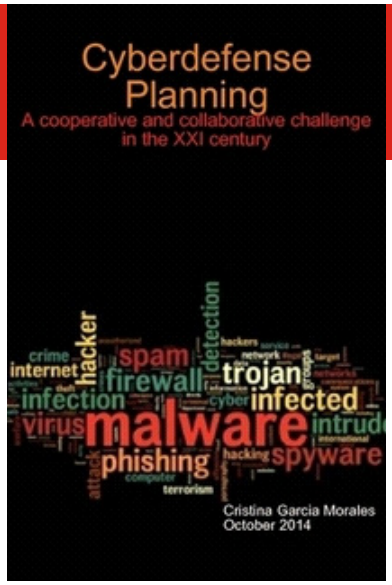
Película:
PRIMER

Sinopsis: Cuatro hombres trabajan en un garaje construyendo aparatos altamente complejos. En parte por accidente y en parte por su pericia, descubren un mecanismo dotado de poderes que les permite conseguir casi todo lo que quieran. Se trata de un hallazgo que podría cambiar el mundo, pero que pondrá a prueba las relaciones entre sus inventores.



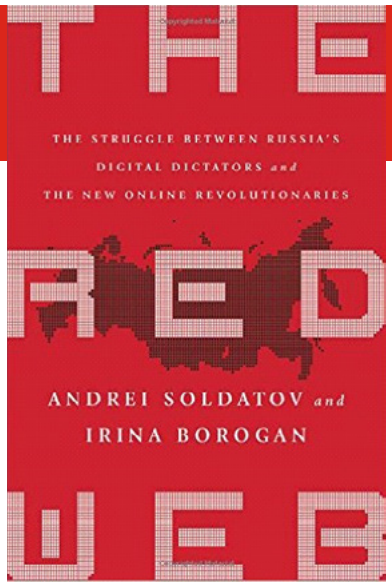
Libro:
EL QUINTO ELEMENTO

Autor: Alejandro Suarez Sanchez-Ocaña
Num. Paginas: 267
Editorial: Oneworld Publications
Año: 2015
Precio: 17.95 Euros
Sinopsis: Una nueva contienda mundial ha comenzado y todos somos soldados en las trincheras. El nuevo gran conflicto internacional trasciende todas las fronteras físicas y se libra simultáneamente en cientos de países. El nuevo escenario de la lucha son las redes digitales, el ciberespacio y el iceberg de la gran Internet oculta que no conocemos.



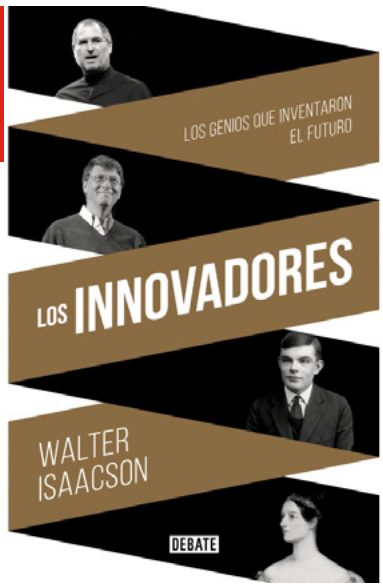
Libro:
CYBERDEFENSE PLANNING

Autor: Cristina Garcia Morales
Num. Paginas: 112
Editorial: Lulu (ISBN- 9781312392151)
Año: 2014
Precio: 6.00 Euros
Sinopsis: El ciberespacio se ha convertido en un elemento clave para el desarrollo social, económico y cultural de las sociedades de hoy en día. La protección del ciberespacio es compleja y requiere una cooperación internacional real con el fin de alcanzar con éxito un nivel aceptable de seguridad a nivel mundial. La autora nos ofrece las claves para hacer efectiva esta colaboración internacional.



Libro:
THE RED WEB

Autor: Andrei Soldatov y Irina Borgoran
Num. Paginas: 400
Editorial: Public Affairs
Año: 2015
Precio: 20.00 Euros
Sinopsis: A partir de decenas de entrevistas con numerosos funcionarios de la Secretaría de Comunicaciones y ciberactivistas que desafían al Estado, Andrei Soldatov e Irina Borogan desentrañan la historia de los sistemas de vigilancia avanzados en Rusia.



Libro:
LOS INNOVADORES

Autor: Walter Isaacson
Num. Paginas: 640
Editorial: Random House Español
Año: 2014
Precio: 16.00 Euros
Sinopsis: Sin llegar a ser una biografía de los principales actores de la innovación TIC, este libro repasa todas las innovaciones, pequeñas y grandes, que han intervenido a crear el concepto y mercado actual de la informática y la tecnología.

7.2 Webs recomendadas

https://www.ncia.nato.int/
Sitio web de la NATO Communications and Information Agency.

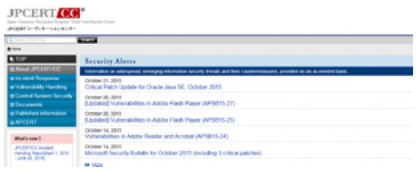
https://www.ncsc.nl/
Sitio web del Centro Nacional de Ciberseguridad de Holanda.

https://nccoe.nist.gov/
EL NIST aloja el Centro Nacional de Excelencia en Ciberseguridad de los Estados Unidos.

http://cybercoe.army.mil/
Sitio web del Centro de Excelencia en Ciberdefensa del U.S Army.

https://cybercamp.es/
Sitio web de evento de ciberseguridad organizado por Instituto Nacional de Ciberseguridad (INCIBE).

https://www.jpcert.or.jp/english/
Sitio web del CERT nacional de Japón.



7.3 Cuentas de Twitter

@rootedcon

@navajanegra_ab

@noconname

@CybercampEs

@hackandbeers

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
3 Nov	Madrid	Symatec	Symantec Day - Advancing Security	https://symantecevents.verite.com/34033/RedSeg
4 Nov	Londres	Cyber Security Expo	Cyber Security Expo	http://www.cybersecurityexpo.co.uk/
4 Nov	Londres	SecurityClearedJobs.com group	Cyber Security Recruitment Expo	http://www.cybersecurityexpo.co.uk/
4-5 Nov	Madrid	ISACA	Jornadas Técnicas 2015 ISACA Madrid	http://www.isaca.org/chapters7/Madrid/Events/Eventos/Pages/Jornadas-Tecnicas.aspx
4-5 Nov	Abu Dhabi	RSA	RSA Conference Abu Dhabi	http://www.rsaconference.com/events/ad15
7-10 Nov	Atlanta	Information Security Forum	26th ISF Annual World Congress	https://www.securityforum.org/events/isf-annual-world-congress
9-11 Nov	Copenague	ISACA	EuroCACS/ISRM - Information Security and Risk Management Conference 2015	https://www.isaca.org/ecommerce/pages/eurocacs-isrm.aspx
10-13 Nov	Amsterdam	Black Hat	Black Hat Europe	https://www.blackhat.com/
14-20 Nov	Washington	Department of Defense Cyber Crime Conf	U.S. Cyber Crime Conference 2015	http://www.usacybercrime.com/main/
17-20 Nov	Viena	DeepSec	DeepSec	https://deepsec.net/
18 Nov	Londres	GovNet Communications	Cyber Security Summit	http://cybersecuritysummit.co.uk/
26 Nov	Madrid	Cloud Security Alliance	V Encuentro de Cloud Security Alliance España	https://www.ismsforum.es/evento/634/v-encuentro-de-cloud-security-alliance-espana/
26-29 Nov	Madrid	INCIBE	Cybercamp	https://cybercamp.es/

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

linkedin.com/groups/THIBER-the-cybersecurity-think-tank