JULIO 2015 / Nº 5

CIBER elcano

REAL INSTITUTO elcano ROYAL INSTITUTE

Desarrollado por:

THIBER

INFORME MENSUAL DE CIBERSEGURIDAD

REAL INSTITUTO
elcano
ROYAL INSTITUTE

Índice

1 COMENTARIO CIBERELCANO:
La ciberdefensa en la Unión Europea

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

A raíz de las crisis de los Balcanes, la **Unión Europea (UE)** procedió a desarrollar una dimensión de seguridad y defensa encaminada a dotarse de capacidades civiles y militares adecuadas para realizar operaciones de prevención de conflictos y gestión de crisis. En poco más de una década, la UE ha construido una arquitectura de seguridad y defensa susceptible de culminar en una defensa común. No obstante, **estos logros en el plano institucional no se han traducido en planes de actuación coherentes y capacidades militares y civiles creíbles**, y no parece probable que esta situación mejore en el corto plazo, tampoco en el ámbito de la ciberdefensa.

En febrero de 2013, Bruselas aprobaba una ambiciosa *Estrategia de Ciberseguridad*, que incluía entre sus principales líneas estratégicas la implementación de un Marco Político de Ciberdefensa (MPCD) que posibilitara la protección de la infraestructura de sistemas de información y comunicaciones que apoyan la estructura, misiones y operaciones de la Política Común de Seguridad y Defensa (PCSD). En este sentido, en noviembre de 2014 el Consejo de Asuntos Exteriores de la UE – siguiendo las directrices marcadas en el Consejo Europeo de diciembre de 2013 – aprobaba la implementación de este marco. Su desarrollo no sólo requiere el protagonismo de los Estados Miembros , la *Agencia Europea de Defensa (EDA)* y la European Union Military Staff (EUMS), sino también de la Comisión Europea – en especial, las direcciones generales de Interior y de Comunicaciones, Redes, Contenidos y Tecnología-, el *Servicio Europeo de Acción Exterior (SEAE)*, la *Agencia Europea para la Seguridad de las Redes y la Información (ENISA)* y la *EUROPOL*.

Las principales acciones definidas en el MPC son las siguientes:

Apoyar a los Estados Miembros en el desarrollo de capacidades de ciberdefensa en el ámbito del PSCD.

Los Estados Miembros deberán participar en el proceso de desarrollo de capacidades en el ámbito del PSCD. Sin embargo, no resultará sencillo. Por un lado, será necesario que éstos posean una visión común de la importancia estratégica de la seguridad y defensa del ciberespacio; y por otro, existen múltiples velocidades en materia de ciberdefensa: algunos países se muestran y mostrarán reticentes a revelar sus cibercapacidades, máxime cuando éstas son sensiblemente superiores a las del resto de sus socios.

"para construir un sistema de ciberdefensa en el seno de UE será necesario algo más que ciberjercicios, adiestramiento y colaboración"

Hasta el momento, la EDA ha llevado a cabo una revisión del *Plan de Desarrollo de Capacidades*, destacando aquellas relacionadas con la ciberdefensa, sobre todo a nivel estratégico, en particular: monitorización, conocimiento de la cibersituación, prevención, detección y protección, compartición de información, capacidades de análisis forense y de malware o lecciones aprendidas, entre otras. En este sentido, la agencia está trabajando en un conjunto de proyectos dentro del *Programa Pooling and Sharing*, entre los que destacan: Sistemas Multiagentes para la detección de APT's (MASFAD), *Cyber Ranges* o el despliegue de *Cyber Situation Awareness packages for headquarters (CySAP)*.

Además, la incorporación de la dimensión ciber en el sistema de planeamiento y misiones de la PSCD supondrá uno de los mayores retos a los que no solo deberá enfretarse la UE sino todos sus EEMM.

Mejorar la seguridad de la infraestructura TIC del entorno de la PCSD en los organismos de la UE.

Algunos países están implementando políticas de '*ciber-higiene*' destinadas a la concienciación en materia de ciberseguridad. En este sentido, SEAE y la EDA lideran un proyecto de similares características que tiene como objetivo minimizar el impacto de las ciberamenazas entre los usuarios de la infraestructura de sistemas de información y comunicaciones que apoyan la estructura, misiones y operaciones de la PCSD, así como proporcionarles directrices claras y concretas para la gestión de ciberincidencias.

Promover la cooperación cívico-militar asi como las sinergias entre el resto de organismos de la UE y el sector privado.

La Comisión, SEAE y la EDA lideran la coordinación y búsqueda de sinergias entre los diferentes actores implicados en la implementación del MPCD. Para ello, la Comisión y la Agencia están llevando a cabo un conjunto de estudios destinados a conocer el estado de madurez de la industria europea de ciberseguridad. Además, la Comisión ha lanzado varios proyectos en materia de ciberseguridad dentro del séptimo programa marco: *CAMINO*, *COURAGE*, *PANOPTESEC* y *CyberROAD*.

Mejorar y fomentar la formación y el adiestramiento en materia de ciberdefensa.

Muchos de los Estados Miembros han desarrollado o se encuentran inmersos en el desarrollo de programas de formación y adiestramiento en el ámbito de su ciberdefensa especifica. El Plan FORCIBE del Ministerio de Defensa español es un ejemplo.

Desde el punto de vista europeo, la EDA trabaja para el fomento de esta formación y adiestramiento. Para ello, ha puesto en marcha múltiples iniciativas, entre las que se encuentran acuerdos con empresas civiles y con otros organismos, como el *Centro de Excelencia de Ciberdefensa (CCD COE)* de la OTAN con los cuales ya ha llevado a cabo seminarios de ciberconcienciacion enmarcados dentro de las actividades de apoyo a la operación EUROFOR RCA.

Mejorar la cooperación con otros actores internacionales.

Una de las prioridades estratégicas de la UE en materia de ciberdefensa es la colaboración con la Alianza Atlántica. Para ello han comenzado ya las conversaciones de alto nivel y se están llevando a cabo un conjunto de acciones. Desde el punto de vista operativo, la EDA ha asumido el rol de observador en el proyecto *Multinational Cyber Defence Education and Training (MNCDE&T)* –liderado por Portugal– del Programa de Defensa Inteligente de la Alianza. Igualmente, el Mando Aliado de Transformación y la Agencia de Comunicaciones e Información de la OTAN han aceptado un rol de observador en el proyecto CyberRanges liderado por la EDA. Además, se está trabajando para que el EU-CERT y NCIRC alcancen un acuerdo –mas allá de un tramite de mínimos– para el intercambio de información técnica y mejorar el proceso de gestión de incidencias. Igualmente, la EDA ha participado como observador en los últimos ciberejercicios –Cyber Coalition y LockedShields– ejecutados por la Alianza.

Fuera del ámbito de la OTAN, la UE trabaja en la promoción de acuerdos bilaterales con otras naciones cibernéticamente avanzadas como Estados Unidos, Corea del Sur, Japón, Rusia, China u ONU.

En definitiva, **para construir un sistema de ciberdefensa en el seno de UE será necesario algo más que ciberjercicios, adiestramiento y colaboración**. Los logros en el plano institucional deberán ir acompañados de: una determinante involucración de los Estados Miembros, una definición clara de las competencias –dejando a un lado sus desavenencias– de los actores europeos implicados, el desarrollo de capacidades de ciberdefensa operativas y planes de actuación coherentes. Bruselas tiene ante sí un extraordinario reto.

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
Hacia una Patriot Act del viejo continente: *quo vadis Europa?*

AUTORES: Angel Vallejo, Responsable de Relaciones Institucionales. THIBER, the cybersecurity think tank. Socio. Maio Legal.
Julia Rubiales, abogada, Maio Legal.

Durante el Gobierno de Jimmy Carter en 1978, el Congreso de los Estados Unidos promulgó la Ley de Vigilancia de Inteligencia Extranjera (Foreign Intelligence Surveillance Act, FISA). La norma establecía procedimientos de vigilancia física y electrónica así como de recogida de "información de inteligencia extranjera" entre potencias extranjeras y "agentes extranjeros", concepto que podía incluir a ciudadanos americanos y residentes permanentes en Estados Unidos, sospechosos de espionaje o terrorismo.

Tras los atentados del 11-S, la Cámara de Representantes y el Senado estadounidense aprobaron, por una abrumadora mayoría absoluta, la USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), que modificaba la FISA y daba carta de naturaleza a otras prácticas de captación y gestión de inteligencia (SIGINT y HUMINT) y establecía amplísimas facultades gubernativas con poco o nulo control judicial previo.

El objeto de la Patriot Act, se dijo, era otorgar mayores facultades a los cuerpos de seguridad e inteligencia, a fin de llevar a cabo todas aquellas actuaciones necesarias para evitar nuevos atentados terroristas. Tales facultades incluían la posibilidad de realizar escuchas telefónicas incluso a ciudadanos americanos, sin necesidad de justificar previamente tal actuación.

A principios de mayo de 2015, la prensa norteamericana e internacional se hacía eco de una sentencia dictada por un tribunal federal de Estados Unidos, que declaraba "ilegal" la recogida indiscriminada de datos telefónicos de millones de ciudadanos americanos llevada a cabo por la Agencia de Seguridad Nacional (National Security Agency, NSA), por exceder lo autorizado por el Congreso en la Patriot Act.

El 31 del mismo mes, el programa de almacenamiento masivo de datos telefónicos quedó teóricamente en suspenso durante dos días. En una apasionada intervención estructurada sobre el uso de la arcaica figura del filibusterismo parlamentario, el republicano Rand Paul se despachó con un discurso de más de diez horas y media, abogando por una radical eliminación de las actividades de la NSA sobre la base que la FISA le otorgaba, y oponiéndose a la mera modificación de la sección 215 de la Patriot Act. A pesar del espectáculo parlamentario, el Senado aprobó el pasado 2 de junio USA Freedom Act (Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring, Freedom Act) que impone límites al programa antes citado y a otros también vinculados a la recopilación de inteligencia y su gestión.

Hoy, con la Freedom Act en vigor, las autoridades gubernativas norteamericanas no tienen ya un campo de acción casi ilimitado en cuanto a las prácticas de la NSA y agencias similares, debido entre otras cosas a la enorme presión ciudadana y a la cuidadosamente estructurada labor de organizaciones como la Electronic Frontier Foundation (EFF). Como consecuencia, los ciudadanos estadounidenses, al menos en teoría, deben estar más tranquilos y asumir que no estarán sometidos a la indiscriminada monitorización de sus comunicaciones por parte del gobierno y sus agencias y de que la intervención judicial debe volver a ser la práctica por defecto.

En Europa, sin embargo, parece que vamos en la dirección opuesta.

Reino Unido aprobó el marzo de este año una ley que exonera de responsabilidad a los servicios de inteligencia británicos, policía y al Centro de Comunicaciones del Gobierno Británico (Government Communications Headquarters, GCHQ) por las actuaciones de hacking que puedan llevar a cabo en equipos ajenos así como por la interceptación de teléfonos sin autorización judicial de cualquier persona, incluso si esta no es aún responsable ni sospechosa de haber incurrido en actuación delictiva alguna.

En Francia, y tras el atentado terrorista de Charlie Hebdo, la Asamblea Nacional elaboró la nueva ley de seguridad y antiterrorismo, que otorga más medios técnicos a los servicios secretos franceses así como una amplia cobertura legal a la hora de interceptar comunicaciones de sospechosos, acceder a redes y bases de datos y obligar a las operadoras de telecomunicaciones a facilitar contenidos sobre sus usuarios. Todo ello bajo control político y administrativo, pero no judicial. El objetivo principal de dicha ley, según el ministro del Interior, Bernard Cazeneuve, es dar a los servicios de inteligencia mayores recursos frente a una “amenaza terrorista grande y seria”.

En España ocurre algo similar. El artículo 18 de la Constitución garantiza, entre otras cosas, el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial en contrario. El domicilio es inviolable, no pudiéndose hacer ninguna entrada o registro sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. También establece que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Sobre dichos principios se ha venido asentando nuestra actual Ley de Enjuiciamiento Criminal (LeCrim) que exige una previa autorización judicial para manipular líneas telefónicas y espiar conversaciones, entrar y registrar domicilios (salvo caso de delito flagrante) y realizar actividades de intrusión en equipos informáticos.

Pero la proyectada reforma de la LeCrim, ahora en debate en las Cortes, ataca la base constitucional y el sistema anterior. En primer lugar, porque permitiría al Ministerio del Interior "pinchar" teléfonos sin autorización judicial previa. En segundo, porque facultaría a las fuerzas de seguridad para instalar programas de los denominados "troyanos" en equipos informáticos o dispositivos electrónicos a fin de "examinar su contenido sin conocimiento de su titular o usuario", sin necesidad, insistimos, de una autorización judicial previa.

¿Quo vadis, Europa? ¿Dónde quedará la tradicional percepción de que el viejo continente actuaba como faro o reducto último de la protección del individuo frente a los tentáculos más intrusivos del poder ejecutivo de sus estados miembros? Europa marcó distancias con los Estados Unidos tras el terrible shock del 11-S, esencialmente en cuanto a los efectos que sobre las libertades fundamentales debía tener la respuesta que habría de darse a los ataques de Nueva York y al estado de (in)seguridad de muchos países occidentales frente a la escalada cualitativa en la amenaza terrorista. Europa apoyó a Estados Unidos, pero no dejó en ningún momento de manifestar que no todo podía valer para intentar enervar el riesgo del terror internacional, ni siquiera el que se había manifestado en su versión más cruenta.

La línea roja (más allá de puntuales autorizaciones o apoyos logísticos de Europa a Estados Unidos muy discutidos por poco transparentes, como los permisos de aterrizaje de aeronaves de guerra en suelo europeo) parecía estar situada en la defensa de los derechos y libertades fundamentales de los ciudadanos así como en la evitación de toda intrusión en el ámbito privado, incluso de aquélla que pudiera provenir de autoridades gubernamentales. Pero ahora varios países europeos, con una coincidencia temporal poco creíble si no se trata de un esfuerzo de cambio coordinado, comienzan a posicionarse en el equivalente (más o menos acusado) a las maniobras legislativas estadounidenses inmediatamente posteriores al 11-S.

De lo anterior se derivan varias preguntas que no deben soslayarse. ¿Cuál es el motivo de que algunos de sus estados miembros afronten modificaciones legislativas que limitan radicalmente los derechos y libertades de sus ciudadanos, otorgando más facultades a sus fuerzas de seguridad para realizar intrusiones en el ámbito privado y, lo que es más importante, sin control judicial?

¿Por qué en Europa se pasa de un espíritu marcadamente liberal en lo que respecta a la salvaguarda de los derechos y libertades fundamentales a otro mucho más permisivo para la autoridad gubernativa, en flagrante perjuicio de sus ciudadanos y, en cambio, Estados Unidos suaviza una postura que inicialmente se identificó con la del ala de los halcones republicanos pero que no ha variado un ápice tras el comienzo de la era Obama?¿Generará esta incuestionable pérdida de derechos de los ciudadanos la muy cuestionable mayor seguridad que pretenden los promotores de las nuevas leyes?

Es muy desasosegante que se intente avanzar legislativamente extramuros del control judicial. Sorprende la consideración implícita de que la actuación de los jueces es incompatible con la eficacia y la rapidez que pueden razonablemente requerir las actuaciones de investigación en casos de terrorismo internacional (yihadista o de cualquier otro corte). ¿No tiene más sentido, si se quiere preservar el espíritu europeo de protección de los ciudadanos frente a las actuaciones de sus gobiernos, dotar al poder judicial de más y mejores medios en vez de simplemente relegarlo a una intervención posterior a las acciones vulneradoras de la intimidad y el secreto de las comunicaciones?

El planteamiento de que la solución a la lentitud o ineficiencia de las actuaciones judiciales es apartar a los jueces del control y toma de decisión de una actuación potencialmente vulneradora de derechos fundamentales es perverso. Si el sistema judicial, en su configuración actual, no puede proteger al ciudadano de alguno de los más graves riesgos a los que éste se enfrenta, habrá que reformar el sistema judicial, y no simplemente trasvasar poder del área judicial al área gubernativa.
Si el proceso continúa, resultará que en Europa habremos clonado con matices la respuesta entonces inmediata (hoy atemperada) que Estados Unidos dio al terror tras el 11-S, pero obviando el contrapeso judicial que los norteamericanos instauraron en su momento.

En efecto, curiosamente, no se vislumbra (en España al menos) una figura equivalente a la FISA Court norteamericana, como elemento ágil, flexible y eficaz de la puesta en marcha de las normas de control de comunicaciones, una suerte de tribunal en alerta las 24 horas del día los 365 días del año a disposición de la autoridad gubernativa que haya podido recopilar indicios suficientes que justifiquen una intervención inmediata que pueda afectar a derechos fundamentales de los ciudadanos.

La situación es muy compleja, y extremadamente preocupante. Europa se desliza, en esta materia, por una pendiente de mimetismo parcial e interesado con las más intrusivas legislaciones de Estados Unidos en el área de las comunicaciones. Es tristemente paradójico que haya que recordar hoy en Europa el adagio de un americano, Benjamin Franklin, según el cual “Aquellos que sacrifican libertad por seguridad no merecen tener ninguna de las dos”.

3 OPINIÓN CIBERELCANO

Ciberreserva:
Una necesidad estratégica para la defensa de la nación.

AUTORES: Enrique Ávila. Subdirector en Centro Nacional de Excelencia en Ciberseguridad (CNEC). Jefe de Servicio de T.I. Área de Operaciones. Dirección General de la Guardia Civil.

Nuestra Constitución, en su artículo 30, determina que:

1. Los españoles tienen el derecho y el deber de defender a España.
2. La ley fijará las obligaciones militares de los españoles y regulará, con las debidas garantías, la objeción de conciencia, así como las demás causas de exención del servicio militar obligatorio, pudiendo imponer, en su caso, una prestación social sustitutoria.
3. Podrá establecerse un servicio civil para el cumplimiento de fines de interés general.
4. Mediante ley podrán regularse los deberes de los ciudadanos en los casos de grave riesgo, catástrofe o calamidad pública."

Tenemos, como ciudadanos, la obligación de participar en la defensa de los intereses nacionales, sin duda, pero, al tiempo, ese deber lleva aparejado el derecho a hacerlo.

El ciberespacio, tal como se manifiesta de forma explícita tanto en nuestra Estrategia de Seguridad Nacional como en la Estrategia de Ciberseguridad Nacional se configura como un nuevo dominio sobre el que ejercer nuestra soberanía como nación. Un espacio que ya no se configura como un territorio físico sino como un complejo entramado de intereses estratégicos que, seamos conscientes de ello, determina, cada vez más, las condiciones de vida del conjunto de los ciudadanos.

Este espacio ya no se comporta como un modelo más o menos reglado por el Derecho Internacional Público y más o menos predecible en lo referente a los actores que en él operan sino que trasciende los conceptos clásicos de soberanía, territorio y, cada vez más, ciudadanía.

Los actores que en el mismo operan no son, únicamente, estructuras políticas clásicas. Ni

tan siquiera son órganos de gobernanza con objetivos determinados, sino que se configuran en un modelo caótico que se asemejaría a una red neural y fractal, muy dinámica. Una red en la que el control sobre los actores intervinientes se hace prácticamente imposible y en la que la importancia de los actores no se encuentra directamente relacionada con su potencia económica o militar sino que ofrece características de asimetría que coadyuvan en la dinamicidad del modelo caótico.

En este entorno tan complejo, intentamos mantener vivos conceptos clásicos de Defensa y Seguridad Nacional que, bajo nuestro punto de vista, han perdido gran parte de su significado. Además de ello, siempre con menguantes recursos económicos y, más trágico aún, con recursos cada vez más limitados en lo que a talento disponible se refiere, por la enorme competencia que generan otros actores.

"Nuestra sociedad se encuentra preñada de talento"

Ese es problema central al que debemos enfrentarnos: Los conflictos en el ciberespacio se configuran como fuertemente dependientes del talento disponible en un determinado momento.

Todo lo antedicho induce una primera pregunta: ¿Nuestras Fuerzas Armadas, en su configuración actual, disponen del suficiente talento para enfrentarse a actores que mueven recursos casi infinitos y que compran el talento o bien disponen de una reserva de talento a la que entrenar si así lo determinan?

La segunda pregunta que hemos de hacernos es: ¿El sistema de carrera profesionalde nuestras Fuerzas Armadas se encuentra adaptado a la posibilidad de un enfrentamiento en el Ciberespacio? Y, en relación con de lo antedicho, ¿se fomenta y se recompensa el conocimiento especializado o se sigue valorando el modelo "oficial para todo" en la creencia de que el adecuado ejercicio del mando suple cualquier carencia de conocimiento?

La tercera pregunta que hemos de hacernos y la que hemos de responder con prontitud es: ¿Existe talento social colectivo y voluntad a la hora de incorporarlo por parte de nuestras Fuerzas Armadas, a la defensa de los intereses comunes, en aplicación del artículo 30 de nuestra Constitución?

Considero que todos, militares y civiles, estaremos de acuerdo en que hemos de responder negativamente a la primera de las cuestiones. Con las carencias, tanto presupuestarias como de reclutamiento y formación de talento especializado de nuestras FAS, no es posible enfrentarse a la tarea de defender el dominio del ciberespacio.

A pesar del esfuerzo realizado con la creación del Mando de Ciberdefensa y a su ciclópeo esfuerzo, este ejercicio de mera voluntad, sin disponer de recursos suficientes, no parece suficiente para salvaguardar los intereses nacionales en este dominio.

Con respecto a la segunda de las cuestiones, consideramos que hemos de introducir mejoras substanciales. Resultar operativo en este dominio requiere una dilatada carrera profesional centrada en un conocimiento especializado que ocupe una parte substancial del currículum del personal destinado a la Ciberdefensa. Desde los soldados y suboficiales, hasta los oficiales.

No podemos, sencillamente, hacer uso de personal extraído de otras unidades y destinado a unidades especializadas en Ciberdefensa. Además de ineficiente, resulta peligroso.

Por supuesto, se ha de recompensar adecuadamente este conocimiento especializado con el fin de hacerlo atractivo para la adquisición de nuevo talento. Hemos de saber recompensar, además del riesgo personal, el nivel de responsabilidad en la protección de los ciudadanos con conocimiento especializado de alto nivel en este dominio.

La respuesta a la tercera de las preguntas sí que nos permite ser optimistas. Nuestra sociedad se encuentra preñada de talento. Mucho de éste se ha puesto a trabajar para aliados y aún para adversarios. Un desperdicio social que ya estamos pagando. Sin embargo, aún nos queda suficiente talento como para dar una respuesta optimista y positiva a la tercera de las cuestiones.

Si convenimos en que lo antedicho es cierto, hemos de pensar en cómo aprovechar para articular al mejor de ese talento del presente y, aún más el talento del futuro, en la participación en la defensa de nuestra nación.

La creación de un cuerpo legal que regule estos derechos y obligaciones en el ámbito de la Ciberdefensa ha de ser un objetivo prioritario de todo gobierno. Una política de Estado de la que, sencillamente, no podemos abstraernos.

Nuestra propuesta, que se ha de configurar desde la lealtad institucional y el respeto mutuo, conlleva la creación y puesta en valor de una estructura paralela de mando y control en la que se ofrezca la participación ciudadana. Un Cuerpo de Ciberreserva. Hombres y mujeres excelentemente cualificados a los que se les deberá ofrecer una pequeña formación militar con el fin de que sean capaces de entender el funcionamiento de una estructura jerárquica de toma de decisión.

Este cuerpo de Ciberreserva habrá de disponer de canales horizontales de relación continua con sus pares militares profesionales para la generación de redes de conocimiento, personal y organizativo, que permitan una integración rápida de ambas estructuras en caso de amenaza.

Al tiempo, habrá de generarse una normativa que regule, de forma clara, sencilla y directa, las competencias de este Cuerpo de Ciberreserva. No es posible optar por el modelo de Reserva Voluntaria actualmente en vigor.

A pesar del enorme fracaso que ha supuesto para España el actual sistema de Reserva Voluntaria; un sistema caduco, inadecuado, ineficiente y más desintegrador que integrador en la defensa de nuestra nación, tenemos la oportunidad de no fracasar en el ámbito de la Ciberdefensa. Existen herramientas tecnológicas que facilitan la colaboración y la compartición de conocimiento. Usémoslas. El objetivo es la defensa de los intereses de España, no lo olvidemos.

Las líneas básicas del modelo que proponemos estarían glosadas de la siguiente manera:

- Estructura de mando análoga a la correspondiente en FAS.
- Establecimiento de sistemas cooperativos de mando y control para entrenamiento.
- Compartición de información para un adecuado despliegue y activación en caso de amenaza o conflicto.
- Generación de un sistema de reclutamiento de nuevo talento.
- Creación y explotación de un sistema de prescripción que permita la primera visibilidad sobre el talento con el fin de competir en su captación en condiciones ventajosas.
- Modelo de integración, en caso de amenaza o conflicto que minimice ineficiencias y competencias indeseadas.
- Definición de un modelo operativo de entrenamiento que permita, mediante el enfrentamiento de competencias, una mejora continua de todos los integrantes de los cuerpos de Ciberdefensa.

CONCLUSIONES

Esta carrera, una carrera de 400 metros, no de 10.000, empezó hace tiempo. Estamos aún en la salida mientras que nuestros competidores están a 300 metros por delante de nosotros. No vamos a ganar. Llegamos tarde. Pero aún tenemos tiempo para clasificarnos para la siguiente ronda.

Ha llegado el momento de superar el nivel estratégico y bajar al barro de los niveles táctico y operativo.

Hemos de equivocarnos con la experiencia. Una y otra vez. Aprender y entrar en un proceso de mejora continua que vaya perfilando, rápidamente y sin pausas, nuestro modelo de participación en la Ciberdefensa de la nación.

Naciones que, en principio, disponen de un campo menor sobre el que reclutar talento o que cuentan con menos recursos económicos o tecnológicos han conseguido realizar un gran trabajo en este ámbito. Nosotros, sin duda, somos capaces de reproducir este éxito, generando un modelo propio.

Cada grupo involucrado ha de cumplir con sus responsabilidades. Ciñéndonos a la creación de un Cuerpo de Ciberreserva, el legislador ha de ponerse en vanguardia y generar un cuerpo normativo sencillo y operativo, alineado con un modelo de sociedad dinámica, que permita la participación del talento ciudadano en la

ciberdefensa de nuestro país. Un Cuerpo de Ciberreserva que se configure como una unidad militar operativa del siglo XXI.

Al tiempo, habrá de arbitrarse un sistema de grados y recompensas que representen adecuadamente ante la sociedad el nivel de responsabilidad de este Cuerpo. En este dominio se abren posibilidades de participación imposibles de reproducir en otros, permitiendo el intercambio de conocimiento entre las partes y el enriquecimiento mutuo.

Dotar, por supuesto, de medios al nuevo Cuerpo con el fin de que, en una primera fase, con el talento ya detectado a día de hoy, devenga en operativo, en un plazo no superior a un año mientras, en paralelo, se ponen en producción los sistemas adecuados para el reclutamiento de nuevo talento entre las nuevas cohortes. Hemos hecho propuestas concretas al respecto que trascienden el objeto de este artículo de opinión.

Por último, operar. Operar en un campo de batalla virtual en el que, permanentemente se realicen juegos virtuales de defensa y ataque. Aprendiendo de cada persona, de cada grupo, de cada situación, de cada dinámica. Y haciendo, en definitiva, que ese conocimiento adquirido se convierta en Inteligencia Colectiva para la Defensa.

Si logramos superar modelos de pensamiento que perdieron su vigencia al final del S. XX y logramos interiorizar que somos una sociedad tecnológica y que nuestra dependencia de las tecnologías de la información, ya sea consciente o inconscientemente, es completa, entenderemos la necesidad de aceptar que hemos de defender el dominio del Ciberespacio con el máximo rigor y la máxima dedicación.

Si logramos vencer nuestra proverbial tendencia hacia la disgregación y la protección de nuestros supuestos derechos corporativos, poniendo el talento común a disposición de la generación de una Inteligencia Colectiva orientada a la defensa de nuestra sociedad, de nuestros ciudadanos, de un modelo de creación de riqueza fuertemente dependiente de la tecnología y de la energía, seremos capaces de diseñar un Cuerpo de Ciberreserva en el que la participación de los ciudadanos en la Ciberdefensa, irrenunciable por lo necesaria, dará como frutos la generación de valor en forma de numerosos intangibles que, en el medio y largo plazo, sin duda, se convertirán en tangibles.

Pensemos, a modo de ejemplo, en la necesaria reindustrialización tecnológica de nuestro país. La dependencia actual en ciertos ámbitos no es deseable, incluso aunque lo sea de aliados confiables. El mayor valor de las sociedades tecnológicas se genera en el ámbito de la I+D+I. Esta participación ciudadana abriría, sin duda, la posibilidad de desarrollar nuevos modelos productivos que, a su vez inducirían multiplicadores de valor en todas las áreas económicas.

Al tiempo, la experiencia civil en los ámbitos relacionados con la Ciberseguridad y con la protección de las infraestructuras físicas se trasladaría a nuestras FAS, enriqueciendo su experiencia y conocimiento en este campo y generando con ello, nuevo valor social.

Competimos contra actores con recursos ilimitados. Necesitamos de todo nuestro talento. También en la Ciberdefensa de nuestro país.

4 Entrevista a Chema Alonso.
CEO de Eleven Paths. Telefonica

1. Como director general de una startup de ciberseguridad española, ¿en su opinión el mercado de inversion nacional en este tipo de empresas está maduro? ¿es sencillo para empresas de nicho españolas acceder a fondos de capital semilla o business angels en las fases iniciales de creación empresarial? ¿y a fondos de capital riesgo para soportar las fases de crecimiento y maduración (serie A, B y siguientes)?

Creo que nuestra experiencia personal no es muy aplicable al resto de las startups de seguridad. En nuestra primera empresa, Informática 64, nuestro objetivo era crear una empresa que nos permitiera trabajar en el área que nos gustaba, que era la informática y en concreto la seguridad informática. Ahora, en Eleven Paths, somos una startup un tanto singular ya que al ser una empresa 100% Telefónica, nuestros fondos de inversión vienen directamente de nuestra matriz. Somos más una "Hot House" que una startup al uso.

Por la experiencia que veo en otras startups como Alise Devices o BlueLiv, con las que tenemos una relación muy estrecha debido a que Telefónica ha invertido en ellas, en España no es demasiado complicado acceder a capitales semilla, pero cuando vamos a rondas de más capital, la cosa se vuelve algo más difícil. Sensiblemente más, si se compara con el mercado extranjero donde la inversión en startups de seguridad vemos que está creciendo a gran velocidad.

2. Actualmente, las políticas estatales de creación empresarial y emprendimiento de ciberseguridad, ¿son suficientes para potenciar y acelerar la creación de un tejido empresarial robusto al respecto? ¿Cree que sería necesario el desarrollo de políticas incentivadoras estatales novedosas para fomentar el emprendimiento en ciberseguridad?

No creo que sea una situación única aplicable para a las startups de ciberseguridad, en términos más generales todas las startups de este país deben afrontar los mismos problemas.

La verdad es que las quejas provienen de cómo se gestionan las obligaciones de las startups desde la Administración Pública y las obligaciones y presión fiscal a las que son sometidos todos los emprendedores al echar a andar su proyecto.

3. ¿Considera que la industria española de ciberseguridad, ya sea de soluciones tecnológicas o de servicios, tiene una madurez adecuada para satisfacer la creciente demanda del mercado, tanto en volumen como en necesidades?

En España, como en casi todos los países del mundo, siguen haciendo falta profesionales de alto nivel técnico en áreas como la ciberseguridad, tal y como sucede en otros campos de especialización como el Big Data, el Cloud Computing o el Business Intelligence. Las primeras potencias mundiales en empresas tecnológicas han fomentado una emigración de talento proveniente del resto de los países, y España no se ha visto inmune a esto.

Ahora mismo, las empresas de ciberseguridad en España se encuentran con un mercado cada vez más maduro, con una inversión en ciberseguridad por parte de todo el tejido empresarial creciente, y con una carencia de profesionales altamente cualificados.

Creo que este ecosistema crea una buena oportunidad para todos los emprendedores que quieran desarrollar su proyecto, ya que hay un mercado de oportunidades. El problema, es la financiación de la que hemos hablado anteriormente y las trabas administrativas, así que si el emprendedor es capaz de solventar estos dos elementos, hay buenas expectativas de éxito para su proyecto.

4. De un tiempo a esta parte parece que existe una tendencia a considerar España como un centro de offshoring de servicios y tecnologías de ciberseguridad, como lo es la India para el desarrollo software: buenos profesionales y baratos ¿Cree que es cierta esa afirmación?

España ha dado grandes profesionales en el campo de la seguridad informática y prueba de ello son la cantidad de ingenieros que actualmente ocupan puestos de responsabilidad en grandes empresas fuera de España. Esta tendencia no parece que vaya a cambiar a corto plazo.

Hay una nueva hornada de jóvenes menores de 24 años que ya están destacando con sus trabajos al respecto. Creo que España seguirá siendo un buen proveedor de profesionales en el área de ciberseguridad para empresas de todo el mundo los próximos años.

5. ¿Cree que España es un jugador de referencia en el mercado de los productos y servicios de ciberseguridad a nivel internacional? ¿Cómo se perciben las tecnologías españolas de ciberprotección fuera de las fronteras?

Este es nuestro talón de Aquiles. Personalmente creo que las tecnologías que hacemos en España aún no han conseguido generar una tendencia en el mercado internacional. En Eleven Paths estamos apostando por ello con productos como Latch, Faast, MetaShield o Tacyt, pero no son muchas las empresas que apuestan por sostener una inversión en producto.

Tenemos grandes éxitos de tecnologías exportadas, como el caso de Virus Total, Alien Vault y los productos de Panda. También algunos productos menos mediáticos pero que llevan largo tiempo traspasando las fronteras en el campo de la ciberseguridad, como son Themida o SmartAccess, y algunas nuevas empresas incipientes en España como el caso de eGarante, BlueLiv o Alise Devices.

No tenemos aún un gran histórico de empresas de éxito en el área de producto de ciberseguridad, pero sí que tenemos experiencia. Lo que necesitamos es consolidar una tendencia consiguiendo que cada día triunfen más compañías.

6. ¿Cómo frenaría la fuga de talento nacional hacia el extranjero?

Yo tengo mi propia teoría al respecto, pero sería largo de debatir. La respuesta fácil es decir que "igualando las oportunidades laborales", pero en muchos casos implica un cambio completo del modelo de país que afectaría hasta los servicios sociales más básicos. Hay países en los que un ingeniero de seguridad puede ganar de 5 a 10 veces más que en España, pero son países con un modelo capitalista más exacerbado. Creo que lo que tenemos que convencer es a los emprendedores de que se puede emprender en España y ponerles las cosas fáciles. Para ello, tenemos que introducir en la educación base de nuestros jóvenes el amor por emprender, de forma que lleven a cabo sus sueños aquí, con nosotros.

7. Ante una potencial situación de indefensión ante ciberataques dirigidos y reiterados, ¿cree que las empresas españolas deberían tener cierta potestad para realizar una "respuesta activa" mediante mecanismos ofensivos para neutralizar el origen del ataque?

Es un tema delicado que debemos afrontar con madurez. La verdad es que no es lo mismo, por ejemplo, bloquear y eliminar la capacidad operativa de un panel de control de una campaña de phishing o de una botnet, que hacer una respuesta activa a un ataque de Denegación de Servicio. La ley a este respecto es a día de hoy clara. ¿Podría una empresa tumbar un servidor porque se sienta atacada en algún modo? Es difícil sacar una regla clara en esos casos.

5 Informes y análisis sobre ciberseguridad publicados en junio de 2015

Cyber Security and Cyber Resilience in East Africa (CIGI y Chatham House)

UK 2015 Cyber Risk Survey Report (Marsh)

Thamar Reservoir (ClearSky)

2015 Information Security breaches survey (UK Government)

Comparison of cybersecurity legislative proposals (US CRS)

Análisis y Caracterización del Mercado de la ciberseguridad en España (INCIBE)

IBM 2015 Cyber Security Intelligence Index (IBM)

Cybersecurity Poverty INDEX (RSA)

6 HERRAMIENTAS DEL ANALISTA: OSRFramework

La proliferación de herramientas destinadas a la monitorización de la actividad en internet es el resultado de la aparición de nuevas formas de utilizar la red en sociedades que se encuentran cada vez más interconectadas. Las compañías tecnológicas han identificado un mercado que demanda de forma reiterada mecanismos que faciliten tanto la detección de posibles actividades fraudulentas como ataques a activos físicos o tecnológicos que, partiendo de la necesidad de atribuir una actividad en internet a una persona, permita identificar posibles usuarios teniendo en cuenta la forma en que se organiza la red.

Pese a ello, no es corriente encontrar soluciones que permitan la identificación de perfiles en múltiples plataformas o la reducción de la complejidad de la identificación de potenciales usuarios de interés cuando se parte de una situación en la que se desconocen los usuarios objeto de estudio pero sí cierta información sobre ellos teniendo en cuenta la idiosincrasia de la estructura de internet.

Las unidades de inteligencia necesitan herramientas que les permitan identificar de forma automatizada la creación de ciertos usuarios en plataformas de internet de cara a poder atribuir una acción que, o bien ha tenido lugar en la red, o bien ha tenido ramificaciones en ella.

Es por esto que *dos analistas e investigadores españoles* han desarrollado *OSRFramework, the Open Sources Research Framework*, una herramienta *opensource* gratuita que permite realizar búsquedas en 236 fuentes diferentes. En función de cuál sea la motivación por la que se quiere monitorizar todos aquellos usuarios que se van dando de alta en una determinada plataforma, las necesidades de búsqueda son diferentes pero la herramienta está diseñada de modo que permite a sus usuarios incorporar nuevas fuentes de forma modular a través de wrappers.

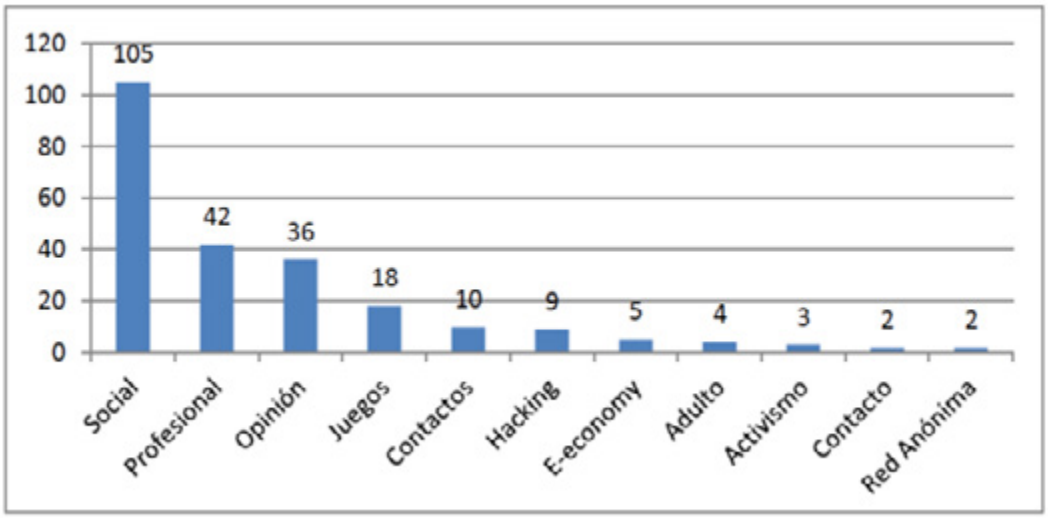


Ilustración 1: Familias de fuentes de búsqueda preconfiguradas en OSRFramework

Obtención de información de API, bases de datos y servicios de terceros

Adicionalmente, se han incluido otras utilidades de terceros que facilitan las tareas de investigación con respecto a determinadas entidades:

De esta forma, OSRFramework permite, como método alternativo a la enumeración de usuarios en aquellas plataformas que permiten la consulta de sus perfiles a partir de índices consecutivos, realizar las siguientes acciones:

- Identificar la existencia de perfiles con un mismo alias. En el caso de disponer de un alias o lista de ellos conocidos de antemano, se puede consultar la existencia de perfiles que los utilicen en todas las plataformas.
- Generar alias candidatos a partir de información conocida. En determinadas situaciones, puede no contarse con un alias dado y disponer solamente de algunos datos del perfil objeto de estudio (como el nombre, apellidos, ciudad, fecha de nacimiento, alias, etc.). Para estas situaciones, la plataforma posee un script que genera una lista de posibles alias a partir de la información suministrada por el usuario.
- Identificar posibles casos de spam telefónico asociados a un número de teléfono.
- Verificar la existencia de información telefónica en internet.
- Identificar la existencia de un correo electrónico asociado a un alias.
- Buscar información sobre cuentas de Bitcoin en la cadena de bloques de blockchain.info
- Consultar si un correo electrónico ha sido filtrado en haveibeenpwned.com
- Consultar la API gratuita de ip-api.com sobre referenciación de direcciones IP y dominios.
- Consultar la existencia de perfiles asociados a personas, emails o usuarios de Skype.
- Generar datos exportables asociados a los resultados a través de transformadas de Maltego.

7 Análisis de los Ciberataques del mes de junio de 2015

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

Como suele suceder con la llegada del periodo estival y de forma continuista con el mes anterior, protagonizado por las mayores fugas de información de los últimos meses, el mes de junio será recordado por dos incidentes de gran relevancia: la aparición de una nueva familia de malware basado en una version renovada de Duqu y la filtración de datos de la *Oficina de Administración de Personal (OPM).*

CIBERCRIMEN

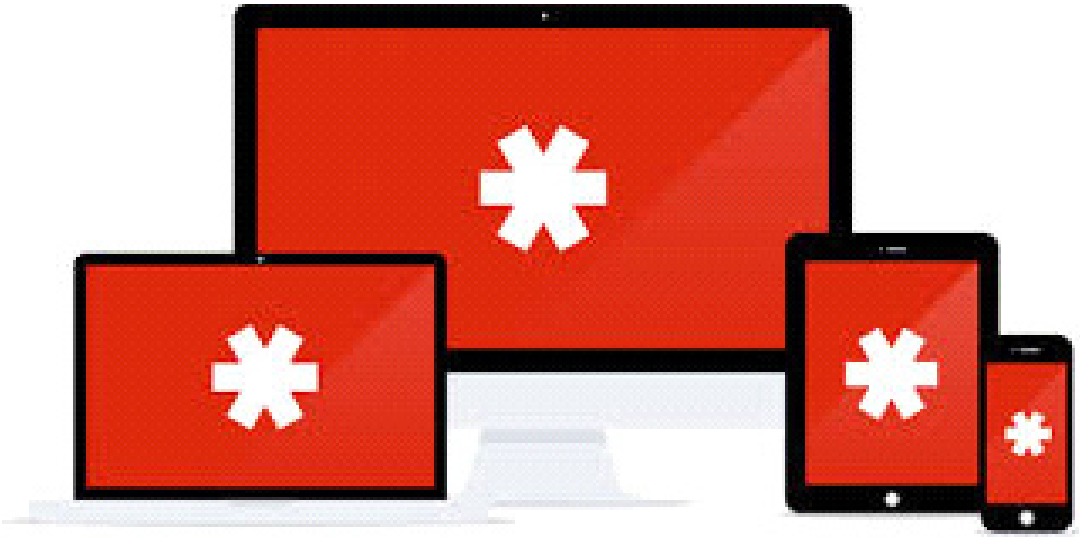
Mientras se sigue especulando sobre la posible autoría tras la fuga de datos La *Oficina de Administración de Personal (OPM)* un dump de la base de datos ha aparecido a la venta en la Deep Web, en el mercado conocido como Hell Dark Market, ofrecida por un usuario cuyo pseudónimo es PING.

Asimismo, el volcado de la base de datos de la OPM ha sido también identificado en otros mercados en la dark web, por lo que se puede observar una gran actividad comercial, lo cual podría llegar a hacer replantearse la motivación tras el ataque, ya que de confirmarse una motivación económica, podría no ser totalmente consistente con las pesquisas iniciales que apuntaban a un autoría estatal por parte de una nación asiática.

No olvidemos que los datos que han sido sustraídos afectan a más de 4.1 millones de registros de empleados federales del gobierno norteamericano que datan desde la década de los 80.

Por otra parte, el popular servicio de gestión de contraseñas en la nube *LastPass ha sido comprometido.* La exposición de datos ha afectado a los nombres de cuentas de usuario, direcciones de correo electrónico, recordatorios de contraseña y hashes de autenticación. Sin embargo, parece que no han tenido acceso a los datos del almacén de usuario cifrados.

Ilustración Volcado de la base de datos de la OPM siendo ofertada en un mercado en la Deep Web



Según la declaración oficial realizada en la página web del servicio, “estamos seguros de que nuestras medidas de cifrado son suficientes para proteger a la gran mayoría de usuarios. LastPass fortalece su algoritmo hash de autenticación con un salto aleatorio y 100.000 rondas PBKDF2-SHA256 ejecutadas en el lado del servidor, además de las respectivas rondas realizadas en el equipo del cliente. Este fortalecimiento adicional hace que sea difícil de atacar a los hashes robados por fuerza bruta”.

A mediados de mes *Trend Micro publicó un comunicado* tras haber descubierto una nueva cepa del malware MalumPoS que fue reconfigurado para comprometer los sistemas PoS basados en la plataforma Oracle MICROS®.

La nueva variante se configuró para golpear esta plataforma de PoS ampliamente desplegada en entornos de restauración y retail (más de 330.000 instalaciones de clientes en todo el mundo).

El pasado 22 de junio, el mercado de servicios cloud mining *ScryptCC ha sido hackeado* y un gran número de Bitcoins fueros robados por un atacante no identificado. En la propia web recomendaban no realizar más depósitos dado que los atacantes han tenido acceso a los hotwallets y a los servidores en una segunda ocasión.

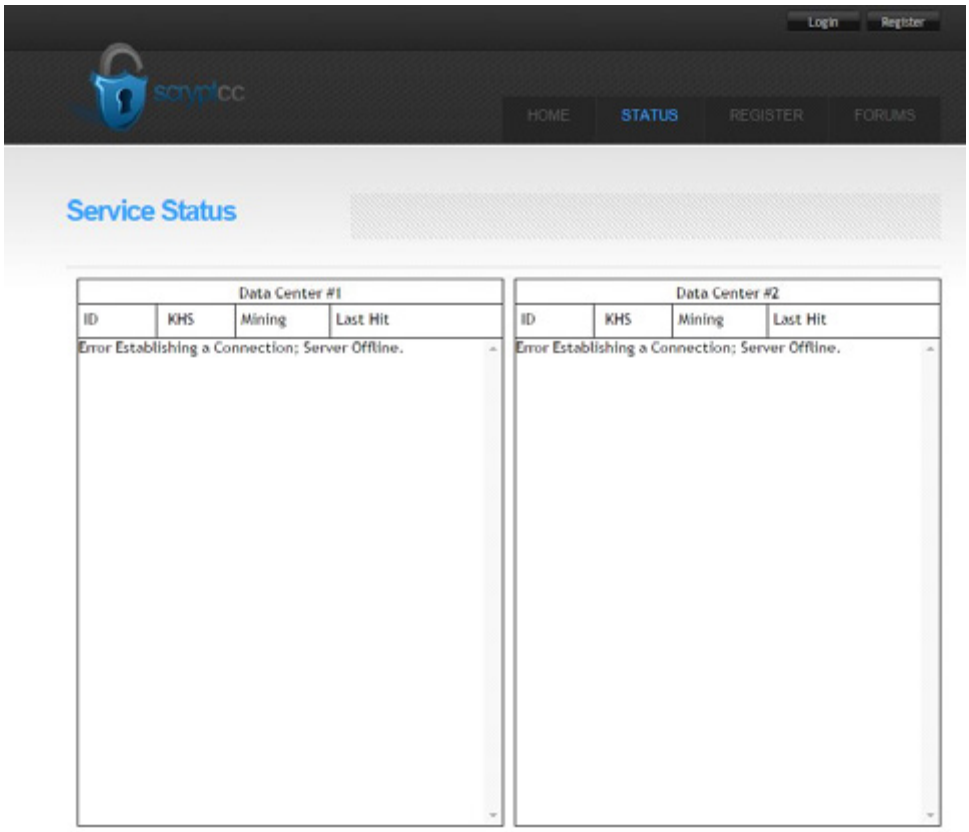


Ilustración: Pantalla que muestra la falta de conexión con el servicio

CIBERESPIONAJE

Durante este mes, la noticia más reseñable en el ámbito del ciberespionaje ha sido puesta en conococimiento por uno de sus afectados, Kaspersky. Una nueva y potente cepa del malware Duqu, denominado *Duqu 2.0*, ha sido descubierta tras desaparecer del escenario en 2012. Duqu 2.0 es un agente muy sofisticado que explota una serie de vulnerabilidades de día 0. Los investigadores de Kaspersky han identificado entre sus objetivos entidades vinculadas a las negociaciones sobre el armisticio nuclear iraní, ya que al menos tres de los hoteles suizos en los cuales se alojaron para mantener las conversaciones de los representantes del G5 + 1, que involucran a EE.UU., Reino Unido, Alemania, Francia, Rusia y China con la UE en relación con la capacidad nuclear de Irán en los últimos 18 meses, se han visto afectados.

También diversas compañías de seguridad TIC han sido infectadas por la misma cepa. Duqu 2.0 también ha afectado a otras entidades en países occidentales, en Asia y en Oriente Medio. Los investigadores de Symantec también detectaron la nueva cepa de malware y observaron infecciones casi en todos los continentes.

La sofisticación del ataque apunta a una autoría estatal con potencial interés estratégico en las conversaciones relativas a las capacidad nucleares iraníes.

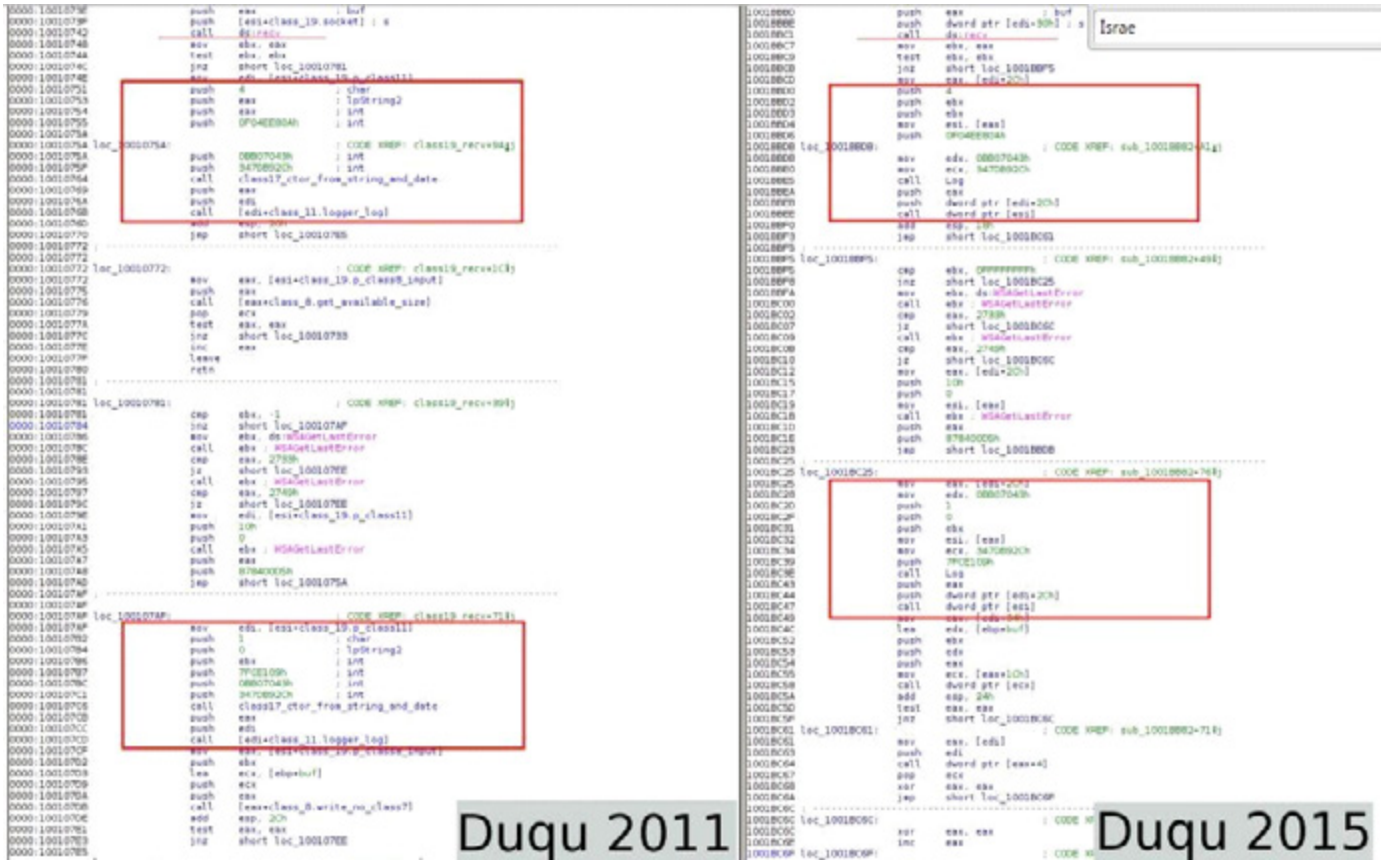


Ilustración: Similitudes entre las cepas de Duqu

A mediados de mes el *Sunday Times* reveló que el Gobierno británico considera que Rusia y China han hackeado los archivos de Snowden, poniendo en peligro las actividades en zona de operaciones de los Estados Unidos y agentes de inteligencia británicos.

Según el *Washington Post*, Snowden sustrajo hasta 1,77 millones de documentos secretos de la NSA, mientras trabajaba para el gobierno de Estados Unidos como contratistas.

La *agencia de noticias británica* citó a altos funcionarios anónimos de los dos servicios de seguridad y el Ministerio del Interior británico, en respuesta a los planes de dichos servicios de inteligencia del Reino Unido para retirar los agentes cuyas operaciones en zona o territorio hostil se han visto comprometidas.

En el anterior número informábamos sobre el ciberataque que afecto a más de 20.000 equipos contra el Parlamento alemán, con una potencial autoría de actores estatales rusos.

No está claro si en esta ocasión se trata de un ciberataque con una nueva motivación criminal o una continuación de los ataques sufridos a finales de mayo. El análisis de GData muestra que se han utilizado nuevas variantes del troyano bancario Swatbanker . La investigación de los archivos de configuración embebidos en el malware muestra que los autores de la botnet Swatbanker integraron nuevas funciones de filtrado para el dominio "Bundestag.btg" (la dirección de la intranet del Bundestag) entre el 8 y el 10 de junio de 2015.

HACKTIVISMO

En cuanto a las motivaciones políticas y activistas, el mes de junio ha estado marcado por el retorno del Syrian Electronic Army (SEA). Tras un breve período de silencio, el SEA ha ejecutado un defacement de la *página web oficial del Ejército de Estados Unidos* y ha añadido un mensaje en una ventana pop-up que muestra el siguiente texto:

"Sus comandantes admiten que están entrenando a las personas que le han enviado a morir luchando."

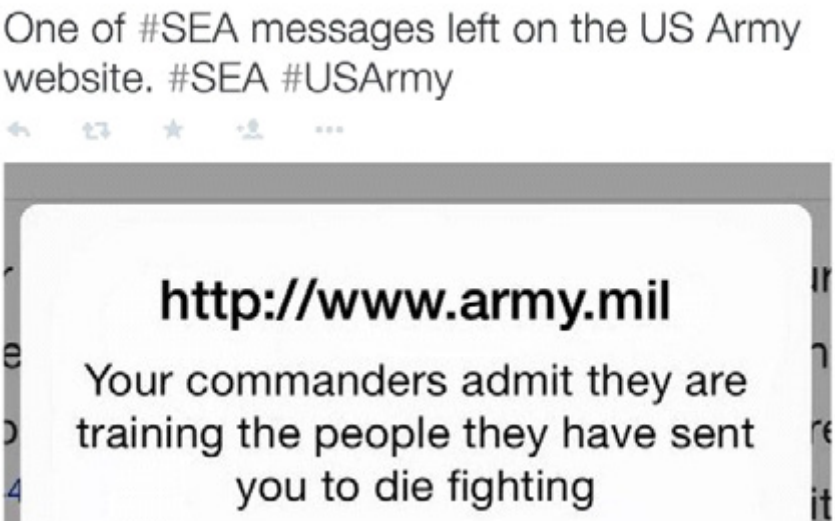


Ilustración Mensaje que aparece en el popup introducido en *www.army.mil*

Los hackers del SEA obtuvieron acceso a la página web a través del sistema de entrega de contenido de Limelight Networks según se desprende de un comunicado oficial realizado por el propio SEA así como de una imagen compartida por el grupo *a través de su cuenta de Twitter.*

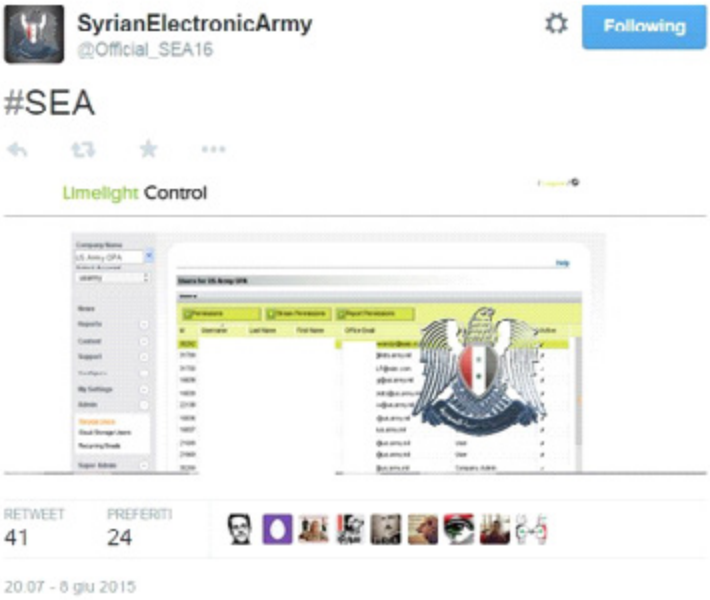


Ilustración Imagen que prueba el acceso al gestor de contenidos de Limelight Network

Al mismo tiempo, el grupo pro-palestino *AnonGhost ha atacado el sitio web oficial del condado de Piatt*, en Illinois, junto con la página web de la oficina del sheriff del condado, la oficina electoral y otros departamentos públicos el pasado 2 de junio.

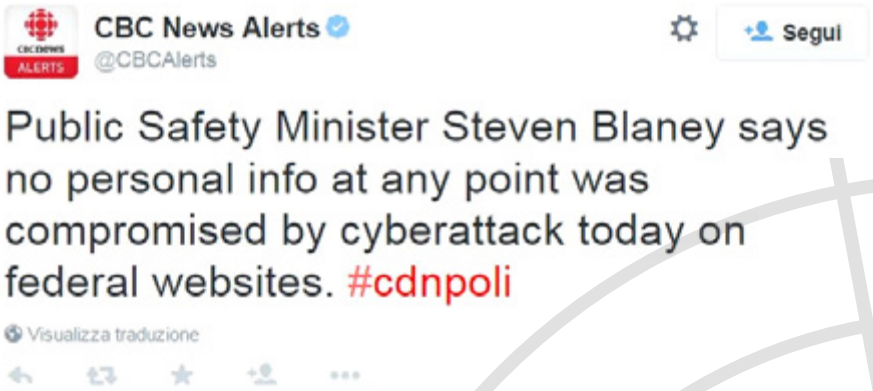
El famoso grupo AnonGhost realizó un defacement en dichos sitios web dejando un mensaje contra el Estado de Israel y en apoyo de la libertad para Palestina. El mensaje también explica la razón de la utilización de la web del condado de Piatt para entregar un mensaje y correr la voz en contra el estado de Israel.

En el *siguiente enlace* se pueden encontrar los links de las páginas afectadas así como los mirrors en zone-h que muestran el defacement.

"WE ARE ANONGHOST WE ARE ALWAYS HERE TO PUNISH YOU ! BECAUSE WE ARE THE VOICE OF PALESTINE AND WE WILL NOT REMAIN SILENT."

El 18 de junio, un ataque de denegación de servicio distribuido (DDoS), atribuido a Anonymous, *paralizaron diversos sistemas y portales del gobierno canadiense* como represalia por el contrario la aprobación de la Ley Antiterrorista C-51.

La operación, *denominada #OpC51* focalizó el DDoS sobre el servidor de dominio gc.ca, que alberga muchos de los sitios web del gobierno canadiense, provocando también la caída de del servicio de correo electrónico utilizadas por el personal gubernamental.

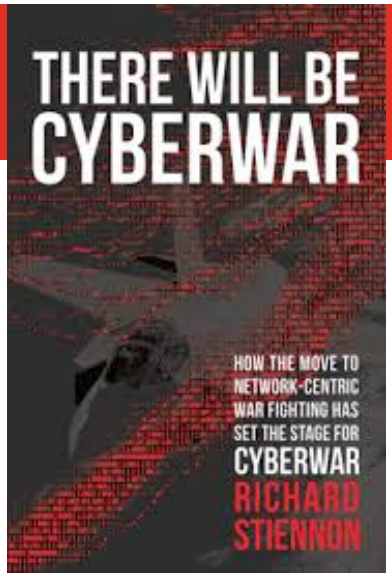


8 Recomendaciones

8.1 Libros y películas

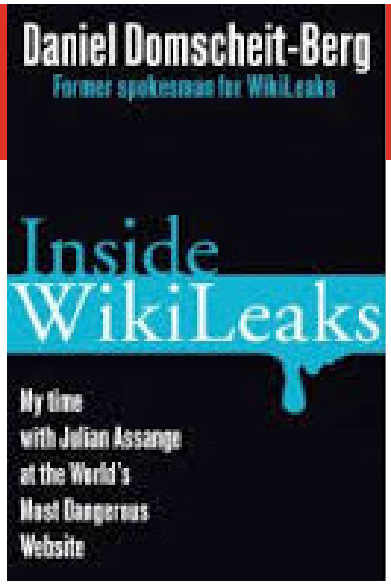
Película:
MATRIX

Sinopsis: ¿Es el mundo lo que parece? Thomas Anderson, programador de una importante empresa de software, de alias Neo, averiguará que no. Con él contactará un extraño grupo encabezado por Morfeo quien le mostrará la verdadera realidad que se esconde tras lo aparente: un mundo dominado por las máquinas, las cuales esclavizan a la Humanidad para utilizar nuestros cuerpos como simple fuente de energía. ¿Pero, y nuestra mente, dónde se encuentra entonces? la respuesta está en Matrix.



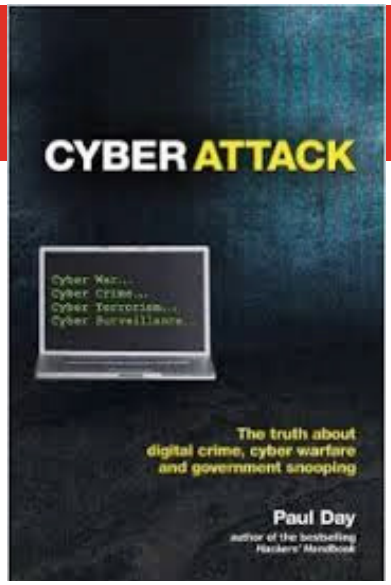
Libro:
THERE WILL BE CYBERWAR

Autor: Richard Stiennon
Num. Paginas: 120
Editorial: IT-Harvest Press
Año: 2011
Precio: 15.00 Euros
Sinopsis: El autor expone como la componente ciber influye, en influirá, en las guerras del presente y el futuro.



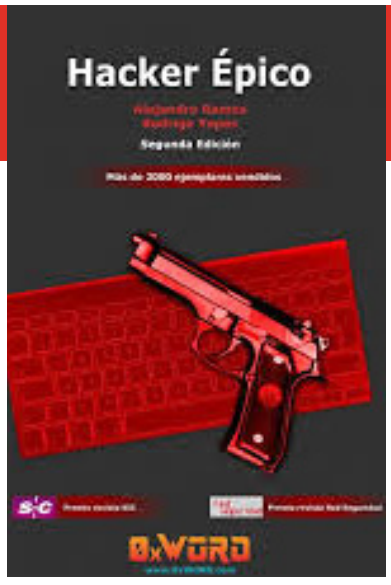
Libro:
INSIDE WIKILEAKS

Autor: Daniel Domscheit-Berg
Num. Paginas: 304
Editorial: Jonathan Cape
Año: 2015
Precio: 15.00 Euros
Sinopsis: El autor, mano derecha de Julian Assange durante los primeros años de Wikileaks, hace un repaso histórico desde los comienzos de Wikileaks hasta su desvinculación del grupo.



Libro:
CYBER ATTACK

Autor: Paul Day
Num. Paginas: 224
Editorial: Carlton Books
Año: 2014
Precio: 20.00 Euros
Sinopsis: El autor, un reconocido experto en materia de ciberseguridad, realiza un análisis de las consecuencias de las nuevas técnicas y tácticas del cibercrimen.



Libro:
HACKER ÉPICO

Autor: Alejandro Ramos y Rodrigo Yepes
Num. Paginas: 256
Editorial: 0xWORD
Año: 2013
Precio: 20.00 Euros
Sinopsis: Mezcla de novela negra y manual técnico, este libro aspira a entretener e informar a partes iguales sobre un mundo tan apasionante como es el de la seguridad informática. Técnicas de hacking web, sistemas y análisis forense, son algunos de los temas que se tratan con total rigor y excelentemente documentados.

8.2 Webs recomendadas

https://www.cybersecurity.ox.ac.uk/
Sitio web del Centro de Ciberseguridad de la Universidad de Oxford.

http://www.mncdet-pt.net/
Sitio web del MNCDET, un proyecto Smart Defence de OTAN destinado a la formacion y concienciacion en materia de ciberseguridad.

http://www.cyberdefensemagazine.com/
Sitio web del portal de noticias Cyber Defence Magazine

https://www.us-cert.gov/
Sitio web del CERT gubernamental de los Estados Unidos

https://www.staysafeonline.org/
Sitio web de la National Cybersecurity Aliance (NCSA) destinado a la ciberprotección.

http://cybersecurity.ieee.org/
Sitio web del Institute of Electrical and Electronics Engineers (IEEE) dedicado a la ciberseguridad.

8.3 Cuentas de Twitter

@STOPTHNKCONNECT

@R_NETSEC

@ICSCERT

@ISMSForumSpain

@OWASP

9 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
1-2 Julio	Guadalajara, México	Expo Tecnología	Expo Tecnología TIC's y Seguridad	http://expo-tecnologia-gdl.com/front_content.php?idart=2&lang=1
1-3 Julio	Lesvos, Grecia	HAISA	International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)	http://haisa.org/
2-3 Julio	Hatfield, Reino Unido	The University of Hertfordshire	14th European Conference on Cyber Warfare and Security ECCWS	http://academic-conferences.org/eccws/eccws2015/eccws15-home.htm
3 julio	Lisboa, Portugal	Bsides	BSidesLisbon 2015	http://www.bsideslisbon.org/
6-8 julio	Madrid, España	UNED / THIBER	Riesgos y amenazas en el ciberespacio	http://extension.uned.es/actividad/idactividad/9445
6-8 julio	Hong Kong, China	ICCIS	International Conference on Computer and Information Sciences	http://iccis-conf.org/
7 Julio	Verona, Italia	IEEE	CSF - Computer Security Foundations Symposium	http://csf2015.di.univr.it/
16 julio	Maryland, USA	NNCoE y NIST	National Cybersecurity Center of Excellence (NCCoE) Speaker Series	https://techcouncilmdassoc.wliinc19.com/events/national-cybersecurity-center-of-excellence-(nccoe)-speaker-series-596/details?dnh=true
20-22 Julio	Alsacia, Francia	IEEE	SECRYPT 2015 - 12th International Conference on Security and Cryptography	http://www.secrypt.icete.org/Home.aspx
22 julio	Singapore	RSA	RSA Conference Asia Pacific & Japan 2015	http://www.rsaconference.com/events/ap14
28-29 julio	Manila, Filipinas	ISC2	Security Congress APAC 2015	http://apaccongress.isc2.org/

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