REAL INSTITUTO elcano ROYAL INSTITUTE

SEPTIEMBRE 2016

Nº 17

CIBERelcano

Informe mensual de ciberseguridad

Desarrollado por: THIBER

Copyright y derechos:

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

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

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

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

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

Informe editado en Madrid.

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank.

Índice

1 Comentario Ciberelcano 04

2 Análisis de actualidad internacional 06

3 Opinión Ciberelcano 10

4 Entrevista a Sergio de los Santos 20

5 Informes y análisis sobre ciberseguridad publicados en agosto de 2016 29

6 Herramientas del analista 30

7 Análisis de los ciberataques del mes de agosto de 2016 33

8 Recomendaciones

8.1 Libros y películas 39

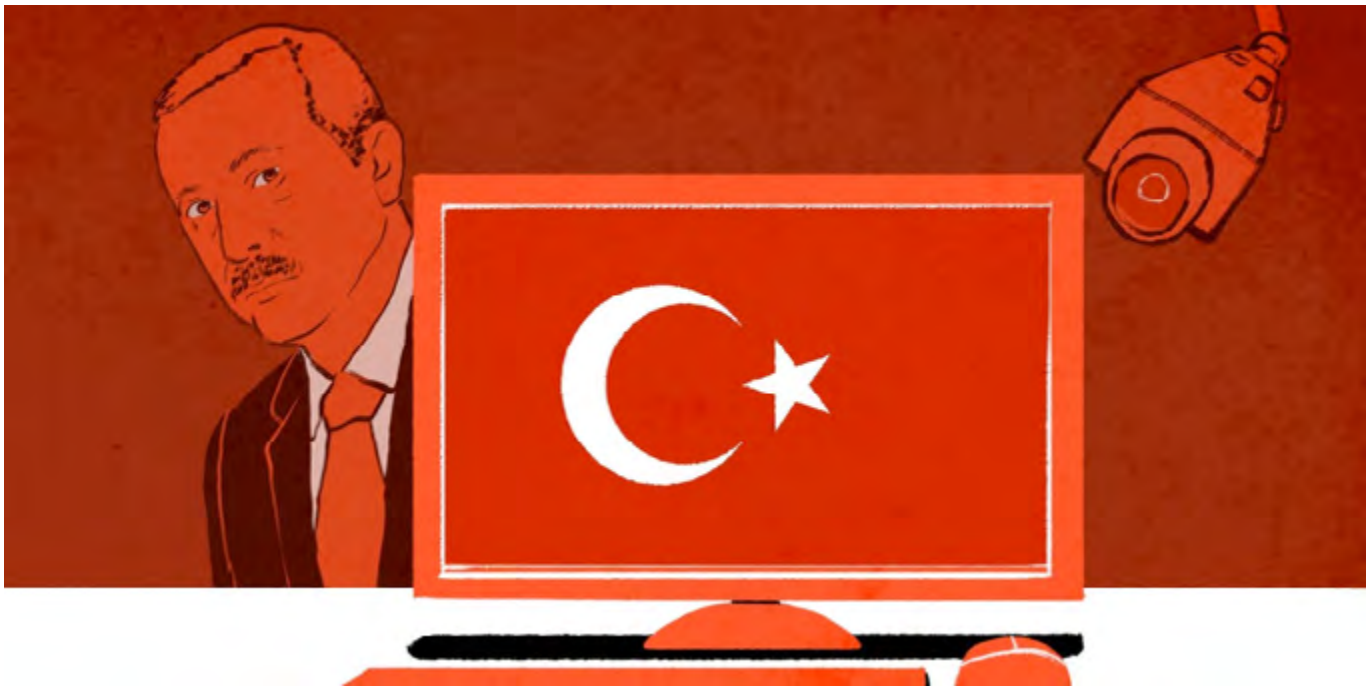
8.2 Webs recomendadas 41

8.3 Cuentas de Twitter.....41

9 Eventos.....42

1 COMENTARIO CIBERELCANO
El control del ciberespacio turco

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



Fuente: Reuters

En mayo de 2013, alrededor del Parque Gezi de Estambul, el pueblo turco se congregó para denunciar el creciente autoritarismo del gobierno de Ankara, las limitaciones a la libertad de expresión y la imparable corrupción que estaba consumiendo al país. Durante estas protestas, el uso de las redes sociales y su poder viral pusieron en jaque al gobierno y, en especial, a Recep Tayyip Erdogan, por aquel entonces Primer Ministro del país. El gobierno asistía atónito al observar como *Twitter, Facebook* o *Youtube* debilitaban el creciente control que ejercía el gobierno sobre los flujos de información que circulaban en Turquía y como el mensaje oficial del ejecutivo quedaba en entredicho.

En septiembre de 2014 el gobierno de Turquía, ya presidido por Erdogan, aprobaba un conjunto de modificaciones a la polémica *Ley 5651*, que habilitaba a Ankara a bloquear cualquier contenido en Internet y acceder a los datos de cualquier usuario sin necesidad de mandamiento judicial. En definitiva, el objetivo era volver a controlar los flujos de información y los mensajes que se transmitían en la Internet turca. En este sentido, fueron muchos los blogueros y tuiteros del país procesados por utilizar Internet para criticar abiertamente la gestión del presidente Erdogan. Del mismo modo, entre febrero de 2014 y mayo de 2015 no sólo se bloquearon más de *80.000 sitios webs*, entre los que se hallaban el controvertido semanario francés *Charlie Hebdo*

o el popular juego en red *Minecraft*, acusado de fomentar la violencia entre los jóvenes turcos; sino que, además, a lo largo del pasado año *el 92% de las peticiones de supresión de contenidos recibidas por Twitter* tuvieron su origen en Turquía.

Desde 2013, la suspensión temporal de los servicios proporcionados por T*witter, Facebook, Youtube, Whatsapp* o *Periscope* ha sido constante, siempre coincidiendo con eventos importantes como elecciones, escándalos de corrupción o manifestaciones en contra del gobierno. No cabe duda del control gubernamental de la red turca, máxime cuando el principal proveedor de Internet del país, *Turk Telekom*, está parcialmente participada por el gobierno de Ankara.

Durante el fallido levantamiento militar del pasado 15 de Julio, Erdogan comprobó en primera persona el poder de Internet. Haciendo uso de *FaceTime* para comunicarse con una periodista del canal *CNN Turkey* fue capaz de movilizar a sus seguidores e impedir que el intento de golpe de estado pudiese haber llegado a buen puerto. La posterior purga – se estima que cerca 80.000 personas, entre militares, jueces y funcionarios, entre otros – fue también posible gracias al control que el gobierno turco ejerció sobre Internet antes, durante y después del golpe.

En definitiva, tal y como ha sucedido con otros mandatarios mundiales, el presidente Erdogan también comprendió en sus propias carnes que el ciberespacio – y más concretamente Internet – es una dimensión configurada para ejercer poder. En este sentido, no es de extrañar que el gobierno de Ankara, ávido por conocer todo lo que sucede dentro de sus fronteras y limitar la disidencia política, emplee la red para ejercer control, proyectar poder e incrementar influencia.

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

Ciberinteligencia: it's all about information

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

CAMBIO DE PARADIGMA

Estamos inmersos en un fuerte proceso de digitalización de nuestro entorno, tanto en nuestro ámbito privado, como en el empresarial y gubernamental. De este modo, cada acción realizada en dichos entornos, tienen una reflexión en el ciberespacio, generando información, procesándola e incardinándola, como si de una reacción en cadena se tratase.

Tanto es así, que las cifras asociadas a Internet desafían la comprensión de las mentes más afiladas debido a su magnitud. En el año 2020, en plena vorágine del concepto de *Internet de las Cosas*, el analista de inteligencia en el ciberespacio deberá tener en cuenta la información generada por los más de 26.000 millones de dispositivos que se estima estarán conectados, tarea a todas luces hercúlea.

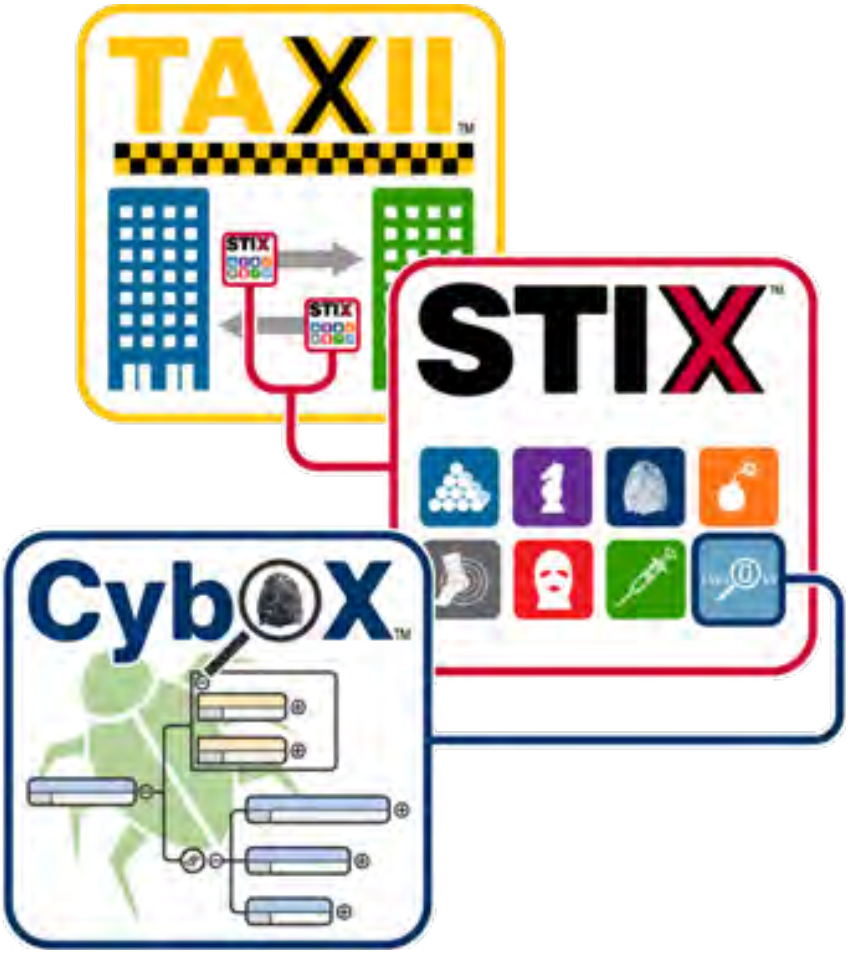
Security Operations Center de la NSA en Maryland

DEFINIENDO CIBERINTELIGENCIA

Según la *definición ofrecida por el Departamento de Defensa de EEUU*, la ciberinteligencia es explicada como "el producto resultante de la recolección, procesamiento, integración, evaluación, análisis e interpretación de la información disponible en relación con las naciones extranjeras, fuerzas o elementos hostiles o potencialmente hostiles, o zonas de operaciones actuales o potenciales".

En términos más coloquiales, podemos afirmar que la inteligencia cibernética no es más que un proceso que trata de recopilar datos digitales, procesarlos e incardinarlos de forma que se genere información de valor que permita apoyar, de forma general, la toma de decisiones en multitud de entornos (como la ciberseguridad), tanto a nivel estratégico, como táctico y operativo.

Así pues, en el ámbito de la ciberseguridad, si bien existen multitud de casos de uso, la inteligencia busca responder preguntas relativas al quién, cómo, dónde, cuándo y el porqué de los ataques, ayudando a diseccionar la comprensión de ciberamenazas presentes y futuras y a realizar esfuerzos prospectivos basados en la inferencia de información existente. Y a su vez buscar que estos esfuerzos permitan anticipar incidentes, identificando amenazas y salvaguardas, vulnerabilidades (y respuesta a las mismas), así como indicadores de actividades maliciosas, permitiendo una postura de seguridad proactiva.



Esquema de intercambio de información de amenazas implementado por el US-CERT

ENTONCES ¿CUÁLES SON LOS RETOS?

Toda esta actividad frenética en el ciberespacio genera datos, una fuente ingente y creciente de información.

Si antaño la dificultad de los analistas era la obtención de información, actualmente lo es la sobresaturación de datos y la "infotoxicidad": tenemos a nuestro alcance, a través de fuentes abiertas y accesibles, más datos de los que podemos procesar.

Así pues, existen literalmente terabytes de datos, no sólo almacenados *(at rest)* sino también en tránsito *(streaming)*, que son extremadamente útiles para el análisis posterior de un evento de seguridad.

Nos encontramos en muchos casos con una necesidad inmediata de resultados que compite con la calidad de la inteligencia generada, evidenciando otro de los problemas que afronta el analista: la velocidad de los datos y su volatilidad. Y es que almacenar la información obtenida de diversas fuentes para procesarla, normalizarla, eliminar duplicidades y agregarla posteriormente, no es siempre una opción cuando el tiempo de respuesta requerido ante un incidente es extremadamente pequeño. Día a día consumimos cada vez más flujos de datos volátiles.

Como consecuencia de la observación de múltiples de fuentes de información, altamente heterogéneas, el analista también deberá sortear el escollo derivado de la coexistencia de datos estructurados (logs, información de antivirus, DLP, etc.) y no estructurados (emails, ficheros, información de redes sociales, etc.)

Por si esto fuera poco, es cada vez más necesario que la ciberinteligencia generada sea "accionable", permitiendo a los usuarios observar sus sistemas para actuar y reaccionar de forma automática ante eventos de seguridad en tiempo real. Para ello, es necesario que el analista y sus herramientas puedan enviar información a otros sistemas en tiempo real, provocando que me-

Uno de los centros de vigilancia 24x7 de la Agencia de Inteligencia de la Defensa norteamericano

diante acciones específicas, denominadas disparadores, los sistemas informáticos receptores puedan actuar en consecuencia, añadiendo por ejemplo reglas a un firewall, actualizando políticas de seguridad o aumentando el nivel general de alerta ante amenazas.

Derivado del punto anterior, la diseminación de la información de inteligencia es una tarea tediosa debido a la falta de normalización de formatos de intercambio de información de amenazas, existiendo diversas iniciativas disjuntas y con diverso grado de madurez y aceptación en el mercado.

CONCLUSIONES

El uso de la explotación de datos del ciberespacio supone un **cambio de paradigma, pasando de una aproximación de seguridad reactiva a una basada en inteligencia,** permitiendo una **postura de ciberdefensa adaptativa** basada en el análisis continuo de información para determinar riesgos y sus impactos.

Así pues, una buena estrategia de inteligencia permitirá arrojar luz sobre la autoría de los ataques, estableciendo relaciones entre sujetos, perfilando actores, permitiendo comprender y comparar las tácticas, técnicas y procedimientos (TTPs) empleados por los atacantes más sofisticados en diversas campañas así como detectar patrones de actividad maliciosa.

La ciberinteligencia no debería sólo estar involucrada en las acciones de ciberseguridad y ciberdefensa. Es una función habilitadora en multitud de ámbitos y con usos aún por definir.

La captura masiva de datos y su almacenamiento derivada de las tareas de observación de fuentes y de enriquecimiento de datos, combinado con el uso de herramientas y técnicas analíticas y de correlación de grandes volúmenes de información (conocido como datasets) puede permitir descubrir los *"unknown unknowns"* a través de técnicas de Big Data Analytics

No hay que perder de vista que, en el ciberespacio, el balance de poder está en el lado del atacante.

"La ciberinteligencia no debería sólo estar involucrada en las acciones de ciberseguridad y ciberdefensa. Es una función habilitadora en multitud de ámbitos y con usos aún por definir… No hay que perder de vista que, en el ciberespacio, el balance de poder está en el lado del atacante."

3 OPINIÓN CIBERELCANO

La incubadora de proyectos de ciberseguridad de la OTAN y otras iniciativas internacionales

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

Jose Ramón Coz, Analista Internacional de THIBER.

RESUMEN

En el presente artículo describimos brevemente las características principales de una de las iniciativas más importantes de la OTAN en ciberseguridad. Se trata de la incubadora de proyectos encuadrada dentro de los esfuerzos que está realizando la Organización en su asociación con la industria y el entorno académico para los temas relacionados con la ciberseguridad (NICP – NATO-Industry Cyber Partnership). En los últimos años se han puesto en marcha una serie de iniciativas en este campo que han cobrado una gran relevancia y en la actualidad constituyen los pilares de la innovación e investigación en ciberseguridad dentro de la OTAN. De manera similar, los países más desarrollados en este campo y diversas organizaciones internacionales están llevando a cabo programas y proyectos de gran alcance que conllevan el desarrollo de iniciativas similares. Por su grado de ambición destacamos en este artículo esta iniciativa, aunque también explicamos brevemente algunos de los esfuerzos multinacionales más destacados.

EL NUEVO ESCENARIO DE CIBERSEGURIDAD

En la Cumbre de Varsovia de la OTAN, celebrada recientemente en julio de este año, la alianza ha reconocido oficialmente el ciberespacio como un dominio operativo militar. Esto significa que la Alianza reconoce el valor estratégico de este entorno y la importancia de que los aliados se defiendan en el mismo de las amenazas existentes.

El ciberespacio forma ya parte de los dominios en los que se desarrollan las operaciones militares y tiene como retos principales la dificultad en la atribución de los ataques y la falta de territorialidad, formando un espacio propio e independiente de las fronteras físicas. La Alianza no descarta la respuesta con armas convencionales o cibernéticas en caso de un ataque en el ciberespacio que causase un grave impacto para los intereses de los aliados, aunque con la prudencia que ha caracterizado a la Organización en sus 67 años de historia respecto a la invocación del artículo quinto del Tratado de Washington.

La dependencia tecnológica de los países y las acciones en el ciberespacio en combinación o como preparación de otras acciones cinéticas, confirman que este dominio es un nuevo campo de batalla. Un ciberataque contra la infraestructura crítica de uno de los estados miembros de la OTAN puede tener consecuencias reales fuera del espacio virtual y, por esta razón, se ha considerado esencial la mejora de sus capacidades cibernéticas. Por supuesto, la Alianza reconoce la aplicabilidad de las Leyes y Tratados internacionales en los citados casos.

Una vez que se ha designado el ciberespacio como un dominio operacional, la OTAN está ya realizando un esfuerzo importante en la interoperabilidad de las capacidades cibernéticas de sus países miembros y se espera un mayor enfoque en la formación y la planificación militar, tomando prioridad el desarrollo en los próximos años de una doctrina inexistente en este campo. La defensa cibernética de la alianza seguirá estando integrada en la planificación operativa, sus operaciones y misiones.

"Los ataques cibernéticos presentan un claro desafío a la seguridad de la Alianza y pueden ser tan perjudiciales para las sociedades modernas como un ataque convencional. Nos pusimos de acuerdo en Gales que la defensa cibernética es parte de la tarea principal de la OTAN en la defensa colectiva. Ahora, en Varsovia, reafirmamos el mandato de defensa de la OTAN y reconocemos el ciberespacio como un dominio de las operaciones en las que la OTAN debe defenderse tan eficazmente como lo hace en tierra, mar y aire. Esto mejorará la capacidad de la OTAN para proteger y llevar a cabo operaciones a través de estos dominios y mantener nuestra libertad de acción y decisión en todas las circunstancias. Continuamos con una intensificación de la política de la OTAN en la ciberdefensa y una mayor fortaleza de las capacidades de defensa cibernética, que se benefician de las últimas tecnologías de vanguardia."

La Alianza lleva más de dos décadas llevando a cabo diferentes iniciativas para las mejoras en sus cibercapacidades. Una de las más recientes

La cumbre de Varsovia de la OTAN de julio de 2016. Fuente NCI Agency.

e importantes es la incubadora de ciberseguridad gestionada desde la Agencia de Comunicaciones e Información de la OTAN *(NATO Communications & Information Agency).* El objetivo de la Incubadora es hacer frente a la mejorable agilidad de la Organización para el desarrollo y adquisición de cibercapacidades, con el fin de defenderse de las amenazas más urgentes y emergentes en el ciberespacio.

EL CONCEPTO DE INCUBADORA DE CIBERSEGURIDAD

Uno de los principales valores añadidos de una incubadora de ciberseguridad es la reducción de plazos de adquisición para el desarrollo de cibercapacidades, tratando de obtener procesos más ágiles que los ciclos de vida estándar de desarrollo.

Además, se trata de centrarse realmente en aquellas áreas que son de relevancia para la comunidad de defensa cibernética operativa, el fomento de la competencia en torno a ideas y soluciones creativas e innovadoras y apoyar las actividades de transformación necesarias dentro de la propia organización. Es muy necesario estar al corriente tanto de las nuevas amenazas que van apareciendo como de las herramientas y metodologías que nos puedan ayudar a prevenir sus efectos, detectar su presencia y responder de manera adecuada de forma que la misión pueda continuar. Por ello, la OTAN trabaja en la transición desde el modelo de aseguramiento de la información al modelo de aseguramiento de la misión.

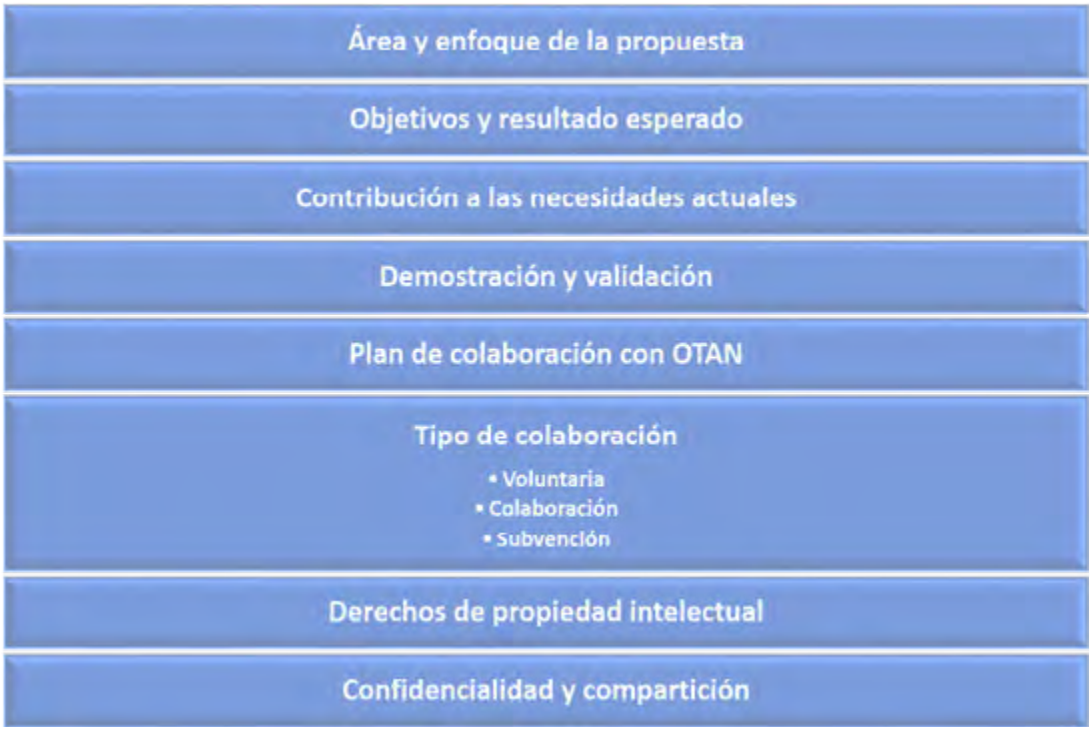
Además, en este caso específico, la incubadora apoya a la industria y las universidades de las naciones que son miembros de la OTAN a

Presentación del proyecto piloto de la incubadora a representantes de la industria y el entorno académico. Fuente NCI Agency.

la que, a su vez, esta iniciativa ayuda a comprender e identificar mejor sus requisitos. Las principales entidades que participan desde la OTAN son el Mando de Transformación Conjunto (Allied Command Transformation - ACT) y la Agencia de Comunicaciones e Información de la OTAN (NCI Agency).

Con el fin de facilitar y promover la colaboración de la incubadora, se han identificado tres posibles mecanismos de colaboración. En primer lugar, las contribuciones voluntarias, en las que los costes son asumidos por la entidad industrial o académica. En segundo lugar, los proyectos de colaboración mediante las contribuciones tanto de expertos OTAN en ciberseguridad como los de la industria y el entorno académico. Por último, el enfoque de apoyo desde la OTAN con la posibilidad de aportación de subvenciones de menor cuantía. La mayor parte de las propuestas (26) se decantaron por las pequeñas subvenciones para cubrir gastos, seguidos por el modelo colaborativo (11) y tan sólo 3 de las propuestas eran voluntarias con los costes asumidos enteramente por el participante y una participación mínima del personal OTAN.

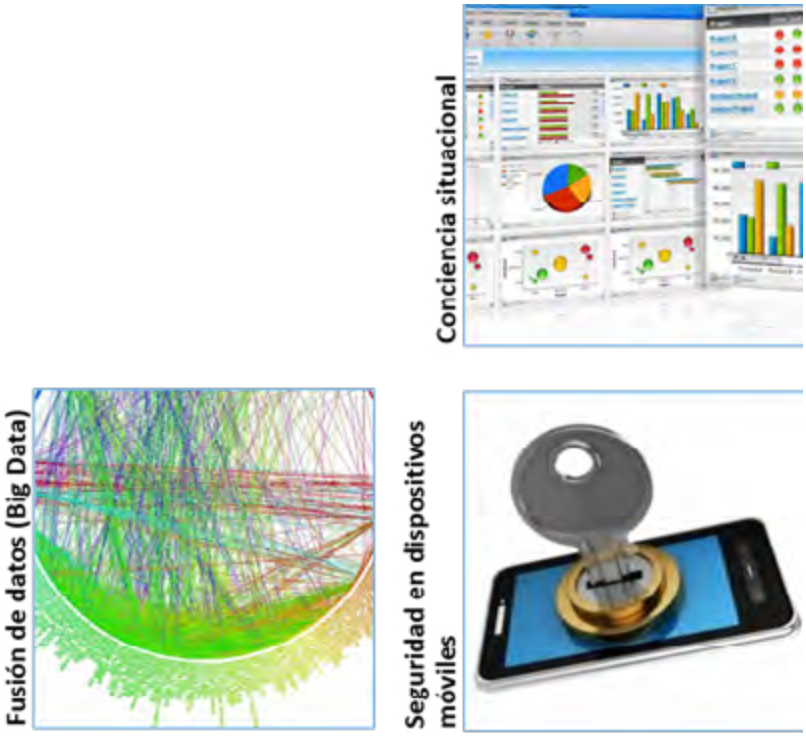
Para las propuestas de innovación, se han considerado relevantes los siguientes puntos.



Consideraciones sobre las diferentes propuestas

La incubadora se gestiona como un programa más, compuesto por varios proyectos. Cada área tiene su propia sección y sus proyectos asociados, que se utilizan para el intercambio de información y para una mayor coordinación con los expertos de la OTAN.

La incubadora de ciberseguridad de la OTAN se puso en marcha en enero de 2015 mediante una fase piloto. Una de las metas de esta fase era estimular el debate y crear el inicio de una colaboración creativa e innovadora entre todas las partes interesadas sobre una amplia variedad de aspectos relacionados con la ciberseguridad. Por otra parte, la fase piloto tenía, además, como objetivo principal definir un marco sobre la colaboración técnica y legal con la incubadora y el establecimiento de un nuevo modelo de negocio asociado. Fueron seleccionadas tres áreas para la fase piloto.



Áreas de enfoque de la Incubadora OTAN

Una vez puesta en marcha la fase piloto, la NCIA recibió unas 40 propuestas sólidas, no sólo de las grandes empresas de Defensa, sino que también participaron entidades de menor tamaño. Esto ha sido uno de los éxitos clave de la fase piloto, ya que al mantener bajos los requisitos de entrada, se ha permitido la entrada y participación de PYMES y Universidades con recursos limitados, pero con un gran potencial para desarrollar las soluciones que la Alianza estaba buscando. Algunos de los participantes remitieron más de una propuesta. 8 participantes eran parte del grupo de grandes proveedores de Defensa, mientras que 21 eran PYMES, 3 eran institutos de investigación y 2 eran universidades.

A través de un proceso competitivo fueron seleccionadas las cinco propuestas más innovadoras en las diferentes áreas. Dentro del área de fusión de datos fue seleccionada la empresa holandesa IntelWorks; en el área de conciencia situacional de ciberdefensa, la empresa francesa THALES y en el área de seguridad en dispositivos móviles fueron seleccionadas la Universidad de Génova, la empresa americana Hewlett-Packard (HP) y la británica PQ Solutions Ltd.

Algunos de los resultados obtenidos fueron presentados en el simposio anual NIAS2015, en septiembre de 2015 en la ciudad de Mons, Bélgica. La fase piloto ha dado lugar a un informe con recomendaciones para las actividades de seguimiento.

PRINCIPALES RESULTADOS DE LA INCUBADORA OTAN

Al tratarse de un proyecto piloto, los principales resultados obtenidos por la Organización han sido una serie de lecciones identificadas que pueden guiar el futuro de iniciativas similares de innovación. Esto, por supuesto, aparte de los resultados específicos obtenidos de cada una de las cinco iniciativas que fueron seleccionadas.

Los objetivos principales que planteaba obtener y alcanzar la fase 1 correspondiente al proyecto piloto eran:

- Un conjunto inicial de necesidades e ideas identificadas sobre innovación en ciberseguridad.
- Una descripción de los procesos de innovación y mecanismos de colaboración validados.
- La visión, misión y estrategia para la incubadora de ciberseguridad de la OTAN.
- Una estimación del esfuerzo y los gastos necesarios para la fase 2.
- Lanzamiento de proyectos prometedores de innovación en ciberseguridad.
- Un portal de colaboración virtual.

El principal logro de este proyecto piloto es que ha permitido a la Alianza y a sus socios del sector privado obtener mayor claridad respecto al punto de vista de cada una de las partes en relación con los retos específicos de ciberseguridad y, al mismo tiempo, ha posibilitado a la industria entender el contexto en el cual opera la OTAN.

PRÓXIMOS PASOS DE LA INCUBADORA OTAN

Una de las propuestas que se está desarrollando es la creación de un intercambiador de innovación con la industria dentro del programa de asociación OTAN-Industria para la ciberseguridad. NICP-X (NATO Industry Cyber Partnership - eXchange) representa un entorno colaborativo en el que expertos en ciberdefensa de la OTAN y de los países miembros, incluyendo industrias, universidades e instituciones gubernamentales aliadas como pueden ser los laboratorios nacionales de defensa, pueden colaborar, fomentar ideas y conocimiento innovador e intercambiar lecciones aprendidas y mejores prácticas.

La propuesta consiste en un laboratorio federado que posibilite la colaboración a las industrias, a las organizaciones de ciencia y tecnología y a los laboratorios nacionales de defensa. El objetivo principal de NICP-X es estimular la innovación mediante un modelo de colaboración federada, en el que las instalaciones nacionales relevantes en las que se desarrollan actividades similares (ensayos, estudios, experimentos, mejoras, pruebas de concepto, desarrollo, interoperabilidad, certificación, etc.) se puedan realizar en un entorno más colaborativo.

"El objetivo principal de NICP-X es estimular la innovación mediante un modelo de colaboración federada"

El modelo desarrollado durante la fase piloto de la incubadora ha sido mejorado para dar respuesta a este nuevo formato basándose en tres pilares principales: la utilización de instalaciones existentes en lo que sea posible, un modelo de operación distribuido y la posibilidad de acceso distribuido.

En principio, y mientras se exploran otras posibilidades, la Red Combinada Federada de La-

boratorios de Batalla *(Combined Federated BattleLab Network* - CFBLNet) puede proporcionar una red experimental protegida con más de 270 nodos reconocidos en 34 países, y que utiliza infraestructuras nacionales y de la OTAN.

OTRAS INICIATIVAS SIMILARES EN EL ÁMBITO INTERNACIONAL

Existen multitud de iniciativas internacionales similares dentro del campo de la ciberseguridad. Una de las que se ha tenido en cuenta durante el desarrollo de la incubadora de ciberseguridad de la OTAN es *Horizon* 2020 de la Unión Europea. Se trata del mayor programa de investigación en innovación de la historia de la Unión Europea. Cuenta con una financiación pública de 80 mil millones de euros disponible durante 7 años (2014 a 2020) a los que habrá que sumar la inversión privada que esta financiación ya está atrayendo y continuará haciéndolo. Promete mayores avances, descubrimientos y primicias mundiales mediante la transferencia de grandes ideas desde el laboratorio hacia el mercado. Entre las secciones de las que se ocupa este programa, podemos encontrar una dedicada exclusivamente al desarrollo de la ciberseguridad y la privacidad digital.

El 5 de julio de 2016, la Comisión Europea ha lanzado la primera asociación europea público-privada para la ciberseguridad. La Unión Europea invertirá 450 millones de euros en esta asociación en el marco del programa *Horizon 2020.* Se espera que los operadores del mercado, representados por la Organización Europea de Ciberseguridad *(European Cyber Security Organisation* - ECSO), inviertan tres veces más hasta los 1.800 millones de euros. La asociación incluirá, además, miembros de las administraciones públicas nacionales, regionales y locales, centros de investigación y universidades. El propósito de la asociación es fomentar la cooperación en las fases tempranas del proceso de investigación en innovación y construir solu-

ciones de ciberseguridad para varios sectores, como pueden ser el energético, la salud, los transportes y el sector financiero.

Como parte del Séptimo Programa de la Unión Europea para la Investigación y el Desarrollo Tecnológicos (FP7), el cuál precedió al programa *Horizon 2020*, podemos resaltar un proyecto llamado IPACSO que ha desarrollado un marco de trabajo en innovación para la seguridad en las tecnologías de la información y las comunicaciones. El proyecto finalizó a finales de octubre de 2015 pero se mantiene ahora como una comunidad con soporte tanto para investigadores-innovadores como para empresas de ciberseguridad, además de para inversores. El marco de trabajo está a disposición de todo aquel que lo quiera utilizar bajo una licencia internacional *Creative Commons* (CC BY-NC 4.0). Entre las muchas actividades que organiza esta comunidad, debemos destacar la organización anual, en octubre de cada año, de los premios europeos de innovación en ciberseguridad y privacidad. Este año celebrarán su tercera edición.

"La puesta en marcha de incubadoras y otras actividades relacionadas con el I+D+i son claves para la implementación y el diseño de nuevas cibercapacidades"

Una iniciativa interesante es la que ha resultado del acuerdo entre el Centro de Investigación Interdisciplinario para la Ciberseguridad *(Interdisciplinary Cyber Research Center* - ICRC) de la Universidad de Tel Aviv y la Asociación Internacional de Transporte Aéreo *(International Air Transport Association* - IATA). Se trata del primer Centro Conjunto en el mundo sobre Innovación en Ciberseguridad para la Aviación. El objetivo principal es promover la investigación y desarrollo en áreas tales como análisis de *big data*, ciberseguridad, autenticación para propósitos de seguridad y comprobaciones sobre seguridad y prevención relevantes para el campo de los vuelos internacionales.

En el área de fuerzas de orden público, el Complejo Global para la Innovación de la INTERPOL (INTERPOL *Global Complex for Innovation* - IGCI) actúa como núcleo para aglutinar las iniciativas nacionales en esta materia. Para luchar contra el cibercrimen con mayor efectividad, la INTERPOL se apoya en las fortalezas y la experiencia de sus países miembros y crea asociaciones estratégicas con entidades regionales e internacionales, el sector privado y las universidades en el campo de la investigación y la innovación en ciberseguridad. IGCI realiza la coordinación de proyectos colaborativos de investigación con el objetivo de desarrollar soluciones informáticas innovadoras y herramientas de análisis e investigación forense digital. El objetivo es mejorar la capacidad de investigación de los crímenes digitales y promover la cooperación entre todas las partes interesadas en este campo. Esta innovación utiliza inteligencia de fuentes abiertas, asociaciones estratégicas con líderes en el campo de la innovación y una gran cooperación con el Centro de Crímenes Digitales de la INTERPOL, donde las

futuras herramientas son ensayadas antes de compartirse con los países miembros.

La puesta en marcha de incubadoras y otras actividades relacionadas con el I+D+i son claves para la implementación y el diseño de nuevas cibercapacidades que han de adaptarse a cada escenario concreto y que deben considerar las limitaciones y, por otro lado, las capacidades nacionales industriales y de investigación. Conscientes muchos países del gran salto tecnológico que en el futuro va a demandar la ciberseguridad, han determinado que no es posible acometerlo sin un enfoque gradual que considere la inversión en investigación y en nuevos diseños y desarrollos industriales innovadores. El que "inventen otros" no es una opción, pues puede crear una dependencia muy importante en muchos ámbitos, no solamente el tecnológico, pues como bien es sabido la ciberseguridad tiene un impacto global en casi todos los campos.

Pero no mencionaremos aquí los países que están invirtiendo miles de millones en ciberseguridad y que, por tanto, pueden acometer proyectos tremendamente ambiciosos en este campo, donde ya la madurez de algunas de las denominadas ciber-incubadoras se ha consolidado. Existen otros muchos países con presupuestos menos generosos e incluso fuera del ámbito OTAN con proyectos muy ambiciosos relacionadas con las ciber-incubadoras. El caso de Israel es ampliamente conocido en el ámbito de la ciberseguridad. Sus grandes inversiones en I+D+i en este campo les han permitido situarse a la cabeza en varios campos de aplicación.

En otros países como Japón, muy unido siempre al I+D+i, el propio gobierno se ha proclamado como la gran incubadora de proyectos relacionados con la ciberseguridad, con inversiones importantes. Otros países, como es el caso de Arabia Saudí está avan-

zando en este campo de forma muy notable, si bien aquí debemos admitir que su presupuesto no tiene nada que envidiar a los líderes mundiales. También podemos poner otros ejemplos más modestos, pero con una gran solidez en cuanto al concepto de ciber-incubadora como Marruecos o Egipto, donde desde sus planes estratégicos cibernéticos han puesto en marcha iniciativas interesantes de las que se pueden obtener lecciones aprendidas para otros muchos países que aún no han puesto en marcha este tipo de proyectos.

CONCLUSIONES

En el presente artículo hemos expuesto el concepto de incubadora de ciberseguridad propuesto por la OTAN, la puesta en marcha de esta iniciativa y los primeros resultados. Además, en el contexto internacional existen muchas iniciativas similares. Hemos destacado algunas de ellas.

Consideramos este asunto clave para el futuro de nuestro país. Existen multitud de iniciativas internacionales que, entendemos, de alguna manera marcarán el futuro en multitud de áreas dentro de la ciberseguridad. Creemos que se debe potenciar e incentivar la investigación y la innovación en estas áreas cuyo crecimiento económico es exponencial. El Estado, la industria y el entorno académico han de trabajar juntos para que los resultados de la investigación se conviertan en productos y servicios tangibles y competitivos en el mercado internacional.

Es esencial realizar un seguimiento de las iniciativas internacionales y por ello desde THIBER se está realizando un trabajo, en el que estamos colaborando, de análisis estratégico sobre el I+D+i en el campo de la ciberseguridad. Posteriormente en otros artículos, iremos desgranando con mayor grado de detalle algunas de estas iniciativas.

4 Entrevista a Sergio de los Santos.
responsable del laboratorio de ciberseguridad e innovación de Telefónica / ElevenPaths

1. Como responsable de un laboratorio de innovación en ciberseguridad ¿podría indicarnos cuáles son los principales objetivos del mismo y las actividades que se llevan a cabo?

Cada uno entiende la innovación de una manera diferente, es una palabra bastante "subjetiva". La innovación se puede referir según quien la defienda a todo el espectro de proyectos que van desde cualquier idea nueva, hasta cualquier planteamiento que se perciba como algo atractivo para el mercado o que el mercado así lo pueda percibir. Los académicos defienden más las ideas "vírgenes" en sí mismas, mientras que en el entorno privado o internet la innovación parece más ligada al éxito o cómo se presente cierta novedad en un entorno. En nuestra área, la innovación se entiende en todas sus vertientes. Tenemos la enorme ventaja de ser transversales a toda la compañía. Podemos plantear desde ideas puramente teóricas (que normalmente pueden acabar presentadas en los entornos más académicos) hasta proyectos mucho más prácticos que acaben en herramientas, productos en sí mismos o mejoras en los productos ya existentes. Esto permite a nuestro equipo experimentar libremente, sabiendo que todo el trabajo será aprovechado de una u otra forma.

Los objetivos más específicos del área de innovación son además capturar y evaluar el talento tanto de compañías como de las personas (Telefónica está apostando fuerte por darle una oportunidad a jóvenes universitarios y em-

prendedores), desarrollar y conceptualizar ideas y exprimirlas durante todo el camino (desde el proceso de creación hasta la posible implementación), establecer alianzas estratégicas con las entidades más punteras para dar salida a su potencial trabajo… En resumen, impregnar todo de nuevas (y esperamos que buenas) ideas, interesantes y por supuesto exitosas si es posible. El laboratorio es el lugar donde se pone todo en práctica, se investiga de una manera más "física", se crean pruebas de concepto, se evalúa y replantean los estándares establecidos, se "depuran" ideas, se conceptualizan y diseñan los prototipos…

Lo cierto es que es un área muy libre donde nos sentimos cómodos para dar más valor en seguridad a todo lo que se desarrolla dentro de una compañía que en principio puede dar la sensación de estar encorsetada. Podemos desde mejorar la seguridad hasta incorporar nuevas

funcionalidades, desde crear nuevos productos a plantear ideas y estudios de investigación… nos relacionamos con muchas áreas diferentes de producto y vamos de la mano con sus planteamientos y necesidades para que la innovación resulte tangible. Aunque en un área de innovación y laboratorio la papelera siempre está llena, pretendemos aprovechar cada paso del proceso creativo y que repercuta en algún área de las muchas en las que colaboramos.

2. En su opinión ¿es España un referente en cuanto a innovación en seguridad?

Para no responder de forma demasiado genérica y vacía, lo dividiría en cuatro partes: personas e investigadores que van por libre, ambiente académico, grandes compañías, y emprendedores.

Quizás no sea una potencia, pero sí que considero que en general tiene mucho que decir al respecto. Desde el punto de vista de las personas y el talento "individual", desde los noventa, donde la seguridad no se encontraba industrializada (y a pesar de no disponer de las mejores infraestructuras), tuvimos buenos investigadores patrios que innovaban en seguridad desde sus habitaciones de adolescentes. Creaban herramientas, métodos y ataques que desafiaban a los profesionales del momento. Hoy, desde un punto de vista más industrializado, contamos con muchos y buenos profesionales que aportan su conocimiento en seguridad a grandes compañías.

Desde el punto de vista académico, considero que no se investiga en seguridad lo suficiente o no se aprovechan esas investigaciones, pero esto no es ningún secreto. Es necesario incentivar a los universitarios para que esas ideas acaben en algo mucho más práctico que un documento al que citar y con el que rellenar currículums. Existen iniciativas para unir el mundo académico con la industria porque precisamente necesitan entenderse mucho mejor en España, algo que en Estados Unidos parecen tener mucho más asimilado.

Desde el punto de vista de las empresas, podemos encontrar buenos ejemplos de innovación en cualquiera de sus definiciones. El hecho de que una compañía como Telefónica haya apostado desde 2013 por la innovación en seguridad como motor de buena parte de su negocio y que posteriormente este modelo haya sido replicado por otras operadoras de telecomunicaciones mundiales que han establecido sus propios equipos de seguridad, es un hecho significativo de que en España se ha ido un paso por delante sabiendo predecir la importancia de esta área en el mercado.

Por último, desde el punto de vista de los emprendedores, se han dado casos muy sonados que han puesto en el mapa a España a nivel mundial en seguridad, pero no percibo un tejido muy tupido en este sentido. La innovación y la apuesta por la creación de empresas claramente orientadas a la seguridad no me parece más o menos numerosa que en cualquier otro ámbito.

"se están creando las mejores herramientas de espionaje e infección, verdaderas obras de arte desde el punto de vista técnico, criptográfico, estratégico…

3. Con una trayectoria de más de 15 años en el mundo de la seguridad informática, con una gran experiencia en el campo del malware y estando involucrado en proyectos como VirusTotal (adquirido por Google), ¿cuál es su opinión sobre el 'estado del arte' en este campo? ¿Realmente estamos asistiendo a una profesionalización y perfeccionamiento de los vectores de ataque? ¿Puede darnos una previsión a corto plazo sobre cómo va a evolucionar?

Lo cierto es que, enlazando con las preguntas anteriores, quien verdaderamente innova de forma práctica, libre y sin ataduras, son "los malos", y la profesionalización no está haciendo más que darles ventaja. Para mí, el campo del malware ha pasado por varias fases. La artesanal, donde la innovación se producía escritorios particulares y la industrializada, hasta la profesional donde los procesos de creación se encuentran ya muy bien engrasados dentro de una maquinaria clandestina que funciona como un reloj. Pero desde hace menos de 10 años ha irrumpido una nueva revolución. La participación de organizaciones gubernamentales con recursos prácticamente ilimitados para moverse en un ambiente sin reglas ni ética, ha permitido que se dispare la inversión en seguridad ofensiva. No es necesario dar explicaciones, no se necesita ofrecer garantías, no hay por qué pedir permiso. Dentro de esta libertad, se están creando las mejores herramientas de espionaje e infección, verdaderas obras de arte desde el punto de vista técnico, criptográfico, estratégico… Si ya la industria del malware resultaba un negocio donde se invertía constantemente en perfeccionamiento y profesionalización (su éxito depende precisa y totalmente de eludir los procedimientos de perfeccionamiento y profesionalización de la otra industria de seguridad), en un entorno con recursos ilimitados el talento y las capacidades se muestran en todo su esplendor. Claro que estamos asistiendo a un nuevo paradigma de mejora. En el momento en el que participan mafias

en el que el componente tecnológico no es más que una de las partes de la rueda de producción, el resto de engranajes obligan a que el vector de ataque o el malware deban estar a la altura. Y si ahí pasamos a un escalón superior donde hablamos de gobiernos… podemos hacernos una idea del nivel.

No sé cómo evolucionará, pero las ciber-armas serán moneda común, creadas por organismos que ayer creaban misiles e innovaban con bombas atómicas. Para el usuario medio, los ataques se extenderán a todos sus aparatos conectados, no solo a sus ordenadores. Hablaremos de ransomware que afectará a toda una casa por ejemplo o a un coche. Veremos quizás extorsiones o robos de identidad no solo físicas sino en redes sociales… sin duda creo que a medida que los atacantes se sienten más particularmente acosados desde un punto de vista técnico gracias a las mejoras en seguridad, se le abren nuevas oportunidades en otros ámbitos más globales.

4. Las empresas de seguridad y fabricantes de tecnologías publican de forma recurrente notas de prensa hablando de programas malware y nuevos vectores de ataque que son desarrollados a diario ¿Es realmente tan cuantiosa la amenaza?

Bueno, hay mucho marketing de por medio, no hay que olvidarlo. Pero la amenaza es real. Las empresas de seguridad y fabricantes aprovechan cada ataque como escaparte para sus productos. Deben siempre estar alerta y mostrar cada ataque como algo novedoso para lo que ellos están preparados. Al usuario menos experimentado, le puede parecer un bombardeo continuo de información desconectada. No terminan de entenderlo y la sensación es de un acoso y derribo de nuevo malware y técnicas innovadoras. Pero para quien está atento, la mayoría de amenazas y ataques son pequeñas variaciones. No por ello menos peligrosas, pero no suponen una verdadera ruptura con respecto a lo que ya conocemos. Obviamente, los grandes cam-

bios se producen cada cierto tiempo. Así que la amenaza sí es cuantiosa, pero la esencia de los grandes problemas de siempre sigue estando ahí: la mayor parte de las amenazas siguen viniendo por la poca concienciación del usuario (él mismo lanza los programas) y a través de la explotación de vulnerabilidades, no hay mucho más. El malware sigue usando las mismas fórmulas de permanencia (puntos de inicio en el registro, servicios, drivers…), etc.

Es curioso como toda esta información debería servir para concienciar al usuario, pero lejos de esto, le provoca impotencia. La seguridad y el malware les parecen incontrolables, un mundo tan incomprensible, cambiante y complejo que acaban por renunciar al más mínimo intento de protegerse más allá del antivirus. En realidad, aunque complejo, a veces pequeñas fórmulas son mucho más efectivas para defenderse. Por ejemplo, durante 2012 y 2013, con eliminar Java del sistema un usuario podía garantizarse una protección más que aceptable. Usar Chrome desde siempre ha multiplicado las posibilidades de salir airoso de un ataque al navegador. Pero nadie les facilita la labor porque Java les es imprescindible para ciertos trabajos o bien Chrome no es compatible con cualquier página. Modificando ciertos permisos en el registro podemos paralizar la inmensa mayoría del malware para que no permanezcan en el equipo… se trata de comprender la naturaleza de las amenazas más que intentar asimilar toda la información caótica y desconectada que se ofrece al respecto. Y pocos usuarios se detienen a asimilar esto, y a la mayoría de los fabricantes y vendedores no les interesa. Hay que esforzarse en que o bien se promocione una cultura más razonada en seguridad, o bien se innove para que la seguridad sea totalmente transparente… aunque no sé qué resulta más costoso y utópico.

"No es ningún secreto, el modelo de Google no está teniendo ningún éxito contra el malware, mientras que el de Apple sí."

5. Con la proliferación de los dispositivos móviles y las recurrentes noticias sobre malware vivo oculto en apps disponibles en los markets (como el reciente y conocido caso de HummingBad) ¿Qué opinión tiene de los markets oficiales de aplicaciones (App Store, Google Play, etc)? ¿Son efectivos para proteger a los usuarios de software malicioso?

No es ningún secreto, el modelo de Google no está teniendo ningún éxito contra el malware, mientras que el de Apple sí. Esto no significa que iOS esté exento de malware o sea perfecto en cuestión de seguridad: aquí únicamente hablamos de cómo se difunde el malware en móviles. Solo hay dos vías: fuera o dentro de los markets oficiales. Fuera de los markets, iOS hace un excelente (aunque restrictivo) trabajo obligando a que su software se firme. Esto limita al malware a encontrar fallos de diseño o vulnerabilidades que permitan instalarlo, pero los atacantes lo consiguen. Dentro de los markets, iOS hace un excelente trabajo igualmente sometiendo las apps a un duro escrutinio. Google es un desastre dentro y fuera, es el modelo consciente que han escogido. Han decidido ignorar la criptografía y

relajar los controles. El resultado ha sido un fracaso, mucho más de lo que el usuario piensa. Y aun así todos siguen lanzando el mensaje de que el uso del market oficial les mantiene protegidos, cosa que no es cierta. El uso del market oficial es recomendable, pero no ofrece ninguna garantía.

6. Con la sofisticación del malware, el estudio del mismo por parte de los analistas se vuelve cada vez más complicado, y las técnicas de ocultación empleadas por los desarrolladores de malware tratando de evitar la detección y el análisis son cada vez más ingeniosas y complejas En su experiencia, ¿cuál ha sido el método que más le ha impresionado?

Es curioso que esta parte sea invisible o poco interesante para la víctima o usuario común, pero aquí es donde reside la mayor parte de la innovación en el malware. A la víctima se la tienen ganada, saben que ejecutará el malware si le convencen, que no habrá aplicado medidas de seguridad avanzadas más allá de disponer de un antivirus, etc… a los malos no les preocupan las medidas que hayan podido tomar las víctimas, saben que no es problema. Pero a los profesionales que los intentan destripar deben sorprenderlos y ganarles en su propio terreno. Y el listón sube a buen ritmo de forma que en esta área se libra una guerra mucho más interesante e innovadora que la que se manifiesta en los medios en forma de alertas para el usuario.

Hay muchas técnicas interesantes que me sorprenden. La más reciente y exitosa consiste en el uso de criptografía estándar en el ransomware para que ningún profesional pueda recuperar la información. Ya apenas cometen fallos a la hora de cifrar los ficheros. Gracias al uso inteligente de la criptografía personalizada en la nube, han conseguido que las consecuencias de una infección de malware sean irreversibles, algo a lo que no estábamos acostumbrados. Pensábamos que, en el peor de los casos, formatear era definitivo, pero cuando el malware captura tus datos esto ya ni siquiera es consuelo.

Por otro lado, en los últimos tiempos, la irrupción de nuevo del malware de macro ha desvelado técnicas muy interesantes e ingeniosas de ocultación, en las que se aprovechan de powershell y técnicas "fileless" (sin tocar el disco). Es curioso como esta fórmula "olvidada" está ganando terreno y ha pillado a los analistas y técnicas de detección casi por sorpresa.

"Aunque parezca contradictorio, los principales problemas de seguridad para los usuarios en internet son la falta y el exceso de información respectivamente "

7. ¿Cuál cree que es el mayor problema de seguridad que enfrentan los usuarios en Internet?

Aunque suene contradictorio creo que son dos: al exceso y la falta de información. Como decía, los usuarios reciben un exceso de información en forma de ruido, intereses comerciales ocultos, información sesgada o directamente errónea. Por otro, es complicado transmitir de forma sencilla la información en seguridad para que el usuario la asimile. Para rematar el problema, el usuario no tiene interés en invertir esfuerzos en seguridad: quiere sentirse seguro con la instalación de programas que lo hagan todo por él, de forma totalmente transparente y sin que requiera de la más mínima interacción. Desgraciadamente encajar el planteamiento así es imposible por definición.

Así que parece que el mayor problema de seguridad consiste precisamente en no entender la esencia de los mecanismos de seguridad en Internet. La información es caótica. Se enfrentan a blogs de empresas que informan, pero también desean vender sus productos, páginas de expertos que en ocasiones bajo el pretexto de la información ocultan un deseo de lucimiento, o de periodistas que con la mejor de las intenciones no han comprendido la naturaleza del problema. Así que el usuario queda perdido entre tanta información, que debe procesar y ordenar. Incluso si lo consigue, es complicado enfrentarse a las amenazas cuando comienzan a ser tan numerosas, sofisticadas e irreversibles como es el mundo del ransomware actualmente.

8. Bajo su punto de vista ¿qué medidas de control o de coordinación echa en falta por parte de las empresas con el objetivo de mejorar la respuesta ante ciberincidentes?

Muchos. No se vigilan adecuadamente que las empresas reporten, remedien y analicen los incidentes. Me llama la atención que todo lo reduzcan a estadísticas de cara a la galería. Hablan de miles de ataques por segundo, sin explicar qué se considera un ataque, y cuántos se han conseguido detener, cuando precisamente los que importan son los que no se han detenido. La realidad es que un ataque serio no se mide precisamente por su velocidad y que puede que el ataque sea tan continuo como silencioso (robo permanente y oculto de información) o escandaloso… pero todos tendrán seguro en común un periodo de incubación y planeamiento por parte del atacante, una etapa en la que es necesario estar especialmente atento a las pequeñas anomalías con las que se delataría un ataque latente.

Además, deberíamos quitarnos complejos y asimilar que el incidente y el ataque van a ocurrir, y por tanto estar preparados. El uso de ciberseguros, en el sentido de pólizas que cubran responsabilidades y obligaciones cuando se produzca uno de estos ataques, me parece el ejercicio de asimilación más sano. Por un lado, una empresa pagará más al seguro si se considera que no toma las medidas oportunas o no se encuentra preparada para mitigar y analizar un ataque, como si se tratara de un conductor negligente. Esto podría ser un catalizador de la cultura de la seguridad. Por otro, disponer de un seguro garantizaría que se dispusiera de recursos para aplicar las medidas reactivas adecuadas dado el caso.

9. Finalmente, ¿qué recomendación realizaría a una persona que quisiese desarrollar su carrera profesional en el ámbito de la ciberseguridad? ¿Por dónde debería comenzar y cómo debería formarse?

Intentaré no decir lo obvio. Creo que lo esencial es igual para dominar cualquier disciplina. Aprender a distinguir el ruido de la paja, y de la información escogida, destilar lo importante. Huir del ruido mediático y acudir a las fuentes más cercanas posibles al origen. Poner todo en tela de juicio, comprobar una y otra vez todas las afirmaciones, indagar y rebatir, exigir pruebas y preguntar por qué. No conozco un ámbito en el que se deba ser más inquisitivo. Resulta demasiado sencillo dar por sentado, seguir patrones sin cuestionarlos o asumir que el otro tendrá la razón y escudarse en ello, creando un clima de confusión y perpetuación de mitos que no aportan nada… cuando realmente creo que muy pocos se preocupan de entender los pormenores y experimentar.

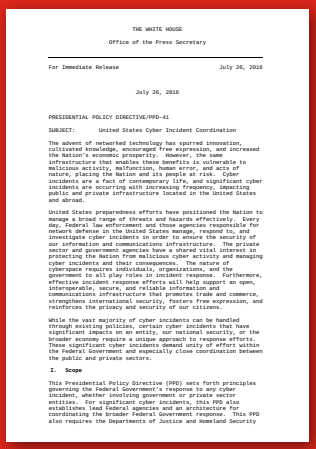
Buscaría la educación reglada (universitaria o de entornos oficiales) complementada con la educación a pie de calle, pero, sobre todo, la formación profesional. Aprovechar el conocimiento que aporta encontrarse en las trincheras de un oficio del que depende tu futuro, prestigio y sueldo. Y siempre expandir tus límites: los programadores deben investigar en seguridad, los investigadores programar, los administradores deberían montar webs, y los que cacharrean a bajo nivel realizar diagramas UML. Invierte tiempo en lo contrario a lo que te dedicas. Es más enriquecedor de lo que parece y paradójicamente un buen motor de aprendizaje en tu propia área, debido a las conexiones y apertura mental que ofrecen.

"Invierte tiempo en lo contrario a lo que te dedicas. Es más enriquecedor de lo que parece y paradójicamente un buen motor de aprendizaje en tu propia área, debido a las conexiones y apertura mental que ofrecen."

5 Informes y análisis sobre ciberseguridad publicados en agosto de 2016

The cost of incidents affecting CIIS (ENISA)

U.S Cyber Incident Coordination Policy (White House)


THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release July 26, 2016

July 26, 2016

PRESIDENTIAL POLICY DIRECTIVE/PPD-41

SUBJECT: United States Cyber Incident Coordination

The advent of networked technology has spurred innovation, cultivated knowledge, encouraged free expression, and increased the Nation's economic prosperity. However, the same infrastructure that enables these benefits is vulnerable to malicious cyber activity. Cyber incidents are a fact of life, placing the Nation and its people at risk. Cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure located in the United States and abroad.

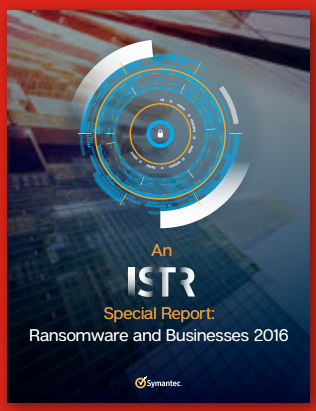
United States preparedness efforts have positioned the Nation to manage a broad range of threats and hazards effectively. Every day, Federal law enforcement and those agencies responsible for network defense in the United States manage, respond to, and mitigate cyber incidents and their consequences, including to our information and communications infrastructure. The private sector and government agencies have a shared vital interest in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences. The nature of cyberspace requires individuals, organizations, and the government to all play roles in incident response. Furthermore, effective incident response efforts will help support an open, interoperable, secure, and reliable information and communications infrastructure that promotes trade and commerce, strengthens international security, fosters free expression, and reinforces the privacy and security of our citizens.

While the vast majority of cyber incidents can be handled through existing policies, certain cyber incidents that have significant impacts on an entity, our national security, or the broader economy require a unique approach to response efforts. These significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors.

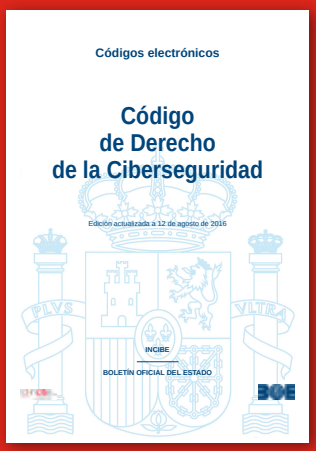
I. Scope

This Presidential Policy Directive (PPD) sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. For significant cyber incidents, this PPD also establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response. This PPD also requires the Departments of Justice and Homeland Security

Ransomware and Businesses 2016 (Symantec)

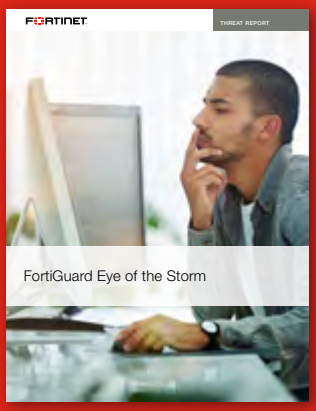


Codigo de Derecho de la Ciberseguridad (Boletin Oficial del Estado)



Medidas de seguridad contra Ransomware (CCN-CERT)

FortiGuard Eye of the Storm (Fortinet)



Tendencias en vulnerabilidades del primer semestre de 2016 (Eleven Paths – Telefonica)

Cyber Primer (UK MoD)

6 HERRAMIENTAS DEL ANALISTA: Laika BOSS

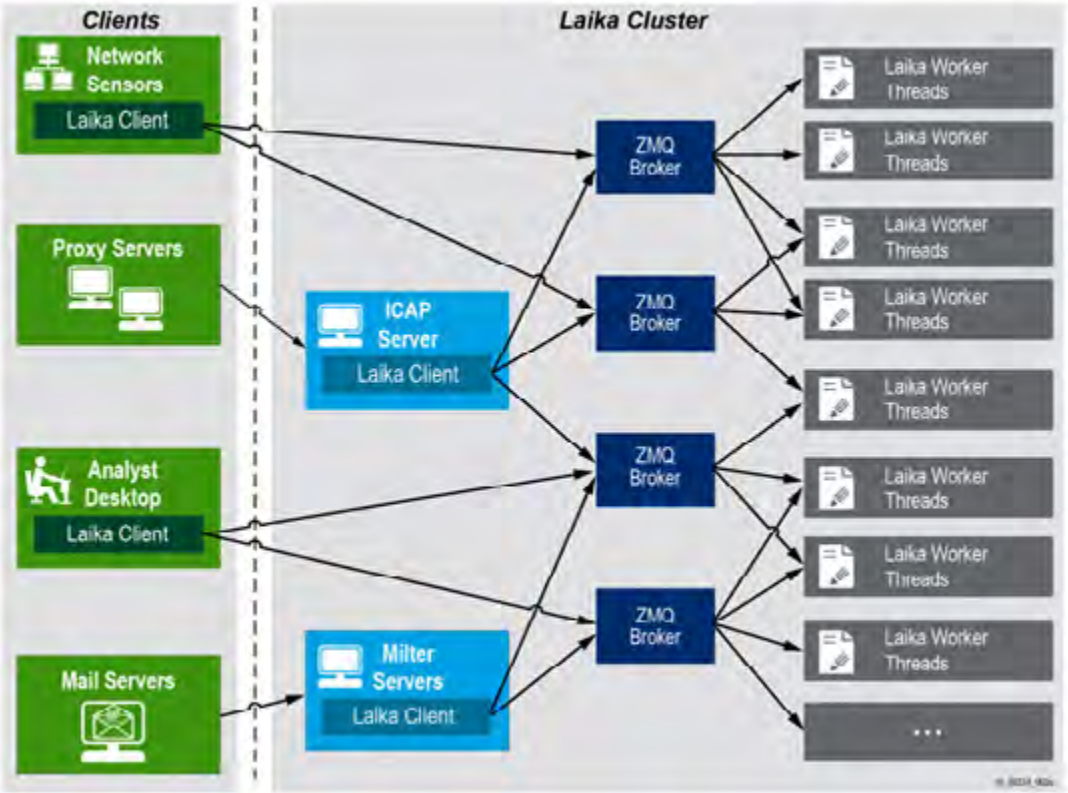
Los atacantes suelen tratar de obtener acceso a una red informática a través de exploits basados en archivos, ya que pueden ser fácilmente entregados e infiltrados en las redes corporativas. Estos atacantes a menudo utilizan los protocolos críticos más comunes como el correo electrónico, web y medios de comunicación social como vectores de diseminación.

La opción más eficaz para frenar ese tipo de ataques suele ser parar los sistemas productivos afectados, conllevando impactos asociados relevantes. Para hacer frente a este tipo de intrusiones, se debería ser capaz de detectar archivos maliciosos dondequiera que existan, ya sea en tránsito por una red informática o en un medio de almacenamiento.

Existe una multitud de herramientas de análisis de malware y para realizar ingeniería inversa. Como resultado, la mayoría de los equipos de seguridad corporativos tienen que gestionar un conjunto dispar de las herramientas de análisis con diferentes capacidades.

Esta solución ineficiente presenta un vector de frustración para muchos profesionales de seguridad que son capaces de detectar malware en un laboratorio, pero no en entornos empresariales en producción.

Laika BOSS es un sistema de detección de intrusiones de seguridad gratuito basado en escaneo de objetos.



Arquitectura del sistema Laika

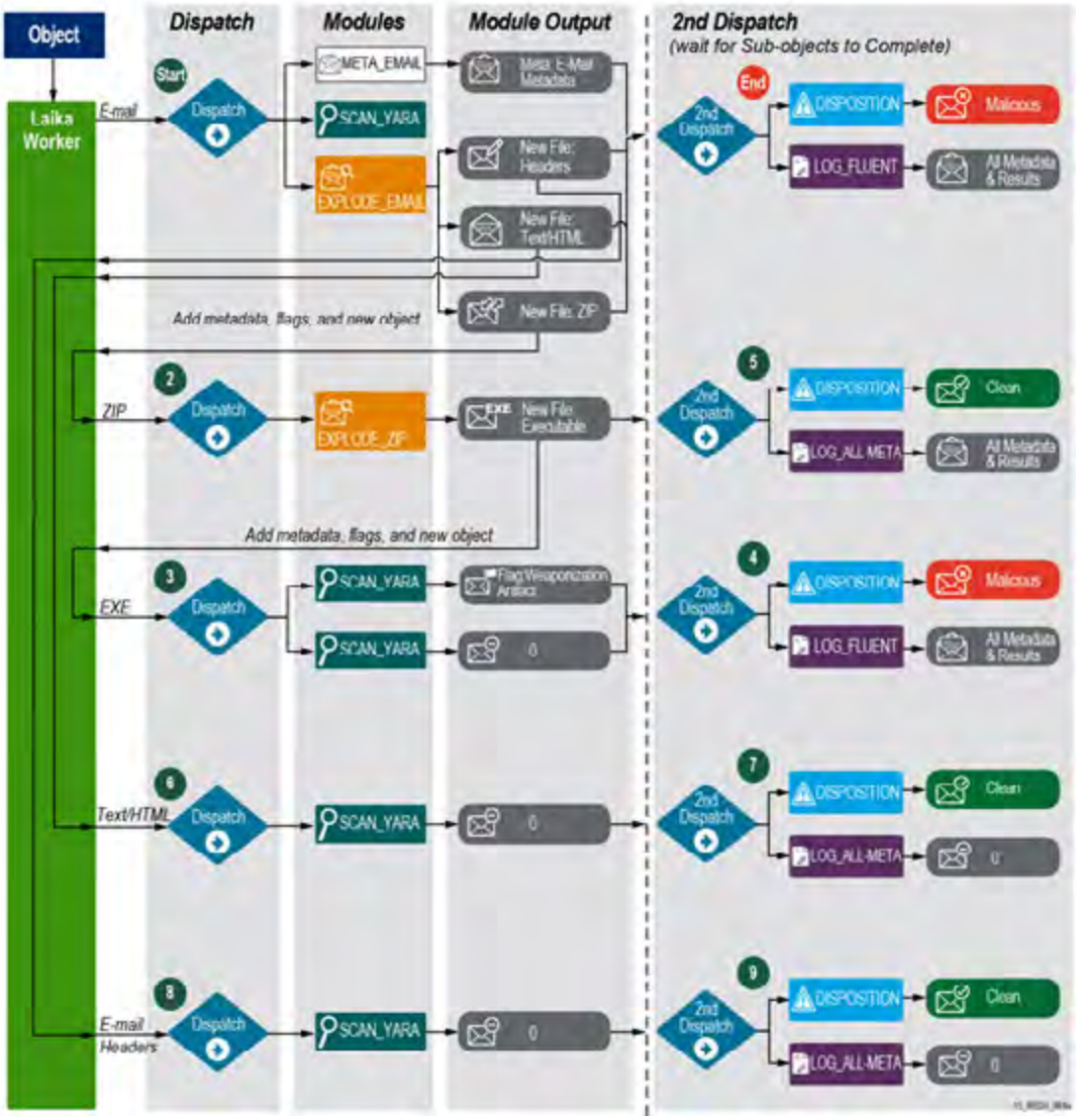
Laika BOSS se basa en proyectos de código abierto, como YARA y ZeroMQ. A su vez, el *framework* IDS de Laika está disponible como un proyecto de código abierto. La colección actual incluye el framework core que incluye módulos y clientes para Milter e ICAP entre otros. También incluirá a corto plazo un cliente para sensores de red, como Suricata. Toda la funcionalidad está testeado en entornos de alto rendimiento y escalable, estando desplegado de forma operativa con éxito en la red global de Lockheed Martin desde el año 2012.

Laika está diseñado para alcanzar los siguientes objetivos:

- **Escalabilidad**
  - o Funcionando a través de múltiples sistemas
  - o Aceptando un alto volumen de fuentes de entrada

- **Flexible**
  - o Arquitectura modular
  - o Lógica de reparto de carga y procesamiento altamente configurable
  - o Inserción de código táctica (sin necesidad de reiniciar el programa)

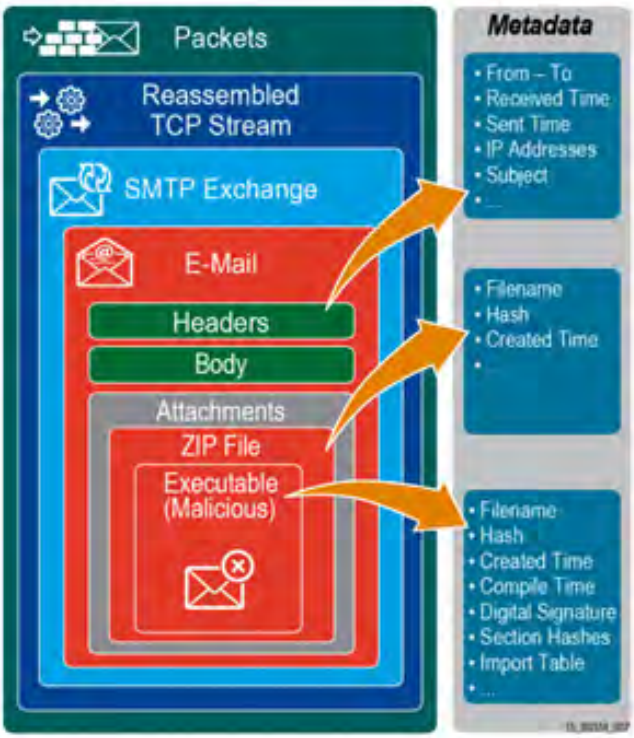
- **Generación de datos**
  - o Permite generar más metadatos asociados a los análisis de los objetos



Dispatcher y ejecución de módulos en Laika

Cada escaneo de objetos ejecuta tres acciones principales:

- Extraer los objetos secundarios: Algunos objetos son archivos, algunos son envolturas, y otros son ofuscadores. En cualquier caso, se encuentran de forma automática a los objetos descendientes del original que deben ser comprobados de forma recursiva mediante la extracción de datos.
- Fijación de marcadores: Los marcadores o flags proporcionan un medio para disponer objetos y para pivotar en un análisis futuro.
- Añadir metadatos: Descubre nueva información empleada para describir el objeto para análisis futuros.



Visión de IDS con Laika de un email malicioso, mostrando un ejecutable sospechoso oculto en un ZIP adjunto

Laika se compone de los siguientes módulos:

- Framework (laika.py): Este es el núcleo de Laika BOSS. Incluye el modelo de objetos y la lógica de dispatching.
- Laikad: Este módulo contiene el código para el funcionamiento de Laika como un servicio local o en red, empleando el launcher ZeroMQ.
- Cloudscan: Es un cliente de línea de comandos para enviar un archivo del sistema local a una instancia de servicio en ejecución de Laika (laikad).
- Módulos: La exploración en sí misma está compuesta por la ejecución de módulos. Cada módulo es un programa en sí mismo que se centra en un subcomponente particular del análisis global de archivos.

7 Análisis de los Ciberataques del mes de agosto de 2016

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

CIBERCRIMEN

Tal vez la acción más relevante en el ámbito del cibercrimen vino dada cuando a mediados de mes un grupo anónimo autodenominado Shadow Broker *publicó lo que parecen ser herramientas sofisticadas de software* que pertenecen a al equipo de élite servicios ofensivos de ciberseguridad vinculados a la Agencia de Seguridad Nacional de Estados Unidos (NSA), conocidos como Equation Group. Un análisis posterior más detallado confirmó el vínculo con el equipo patrocinado por el estado.

```
#!/bin/sh
#
# BG User script:
# Script to set up user env for BG
#
# Changelog:
# 6/23/10 -- Cleaned up script, as well as fixed error with multiple scripts being started
# 7/9/10 -- Changed the format of the log file created
# 7/8/11 -- Changed to support both Blatsting, BG and Bliar
# 11/9/12 -- Changed to support for BUZZLIGHTYEAR
# 3/11/13 -- Added BANALRIDE.
# 5/3/13 -- Changed BANALRIDE ASA location to BG3121.
# 6/11/13 -- Modified layout of disk so TPATHS have been updated...
# 7/25/13 -- Removed blockme rules and added in support for BG3121 as we move to merge
# 8/18/13 -- Updated paths to match the new directory structures
```

Old Equation group malware code	Code from Shadowbrokers' leak

`*(_DWORD *)buf = 0xB7E15163;`
`i = 1;`
 	
`do`
`{`
`*(_DWORD *)(buf + 4 * i) = *(_DWORD *)(buf + 4 * i - 4) - 0x61C88647;`
`++i;`
`}`
 	
`while ( i < 44 );`
	`i = 1;`
	`*(_DWORD *)buf = 0xB7E15163;`
	
	`do`
	`{`
	`*(_DWORD *)(buf + 4 * i) = *(_DWORD *)(buf + 4 * i - 4) - 0x61C88647;`
	`++i;`
	`}`
	
	`while ( i <= 43 );`

Comparación de código software asociado a Equation Group

A primeros de mes, Peace, el hacker que ha vendido anteriormente grandes leaks de credenciales de usuario de MySpace y LinkedIn, *pone a la venta 200 millones de supuestas credenciales de los usuarios de Yahoo* en un market online denominado Real Deal.

De acuerdo a una muestra de los datos fugados, parece contener los nombres de usuario, hashes de las contraseñas (creados con el algoritmo MD5), fechas de nacimiento, y en algunos casos,direcciones de correo electrónico de respaldo. Los datos estaban siendo vendidos por 3 bitcoins, alrededor de 1.860 $, y supuestamente contiene 200 millones de registros de desde el año 2012.

Por su parte la compañía confirma ser consciente de la reclamación del atacante y está tomando medidas al respecto.

Ventra de credenciales robadas de Yahoo

Por otra parte, el grupo Carbanak parece haber comprometido un portal de atención al cliente para las empresas que utilizan el sistema de pago con tarjeta incluido en la solución de punto de venta (PoS) de Oracle MICROS, y *ha sido utilizado para robar las credenciales del usuario administrador implantando código malicioso en 700 de estos terminales.*

Finalmente, *el sitio web oficial de Michael Phelps ha sido el objetivo de unos atacantes* después de que el nadador norteamericano ganase su decimonovena medalla de oro olímpica en los relevos de 4x100 en las Olimpiadas de Río de Janeiro.

El grupo conocido como New World Hackers se ha atribuido la responsabilidad de un ataque de denegación de servicio distribuido (DDoS) que provocó caídas prolongadas de la web.

Página oficial de Michael Phelps durante el ataque de DDoS

CIBERESPIONAJE

En el plano del ciberespionaje, *a principios de mes diversos medios se hacían eco de un ciberataque realizado por atacantes iraníes,* comprometiendo más de una docena de cuentas en el servicio de mensajería instantánea Telegram e identificado los números telefónicos de cerca de 15 millones de usuarios iraníes, lo que es, hasta la fecha, la mayor fuga de información sufrida por dicha plataforma.

Los ataques, que tuvieron lugar en diversos momentos a lo largo de este año, no han sido detectados hasta ahora, poniendo en peligro las comunicaciones de activistas, periodistas y otras personas en posiciones sensibles en Irán, donde Telegram es utilizado por unos 20 millones de personas.

Amir Rashidi, el investigador de seguridad de Internet que ha trabajado con los usuarios de Telegram que fueron víctimas de la piratería, posa para una fotografía en las oficinas de la Campaña Internacional para los Derechos Humanos en Irán

El 7 de agosto, *el equipo de analistas de Symantec reveló los detalles de Strider*, un grupo de atacantes hasta ahora desconocido que ha lanzado diversas campañas de ciberespionaje contra objetivos seleccionados en Rusia, China, Suecia y Bélgica (36 infecciones detectadas en 7 organizaciones desde 2011). El grupo emplea una avanzada pieza de malware conocido como Remsec (Backdoor.Remsec) para llevar a cabo sus ataques. Su código contiene una referencia a Sauron, el antagonista que todo lo ve en El Señor de los Anillos.

```
KBLOG_ROTATE_SECS = 10800
tmp_dir = (os.getenv("WINDIR") .. "\\temp\\"
drive = "C:\\"
SAURON_KBLOG_KEY = "mISfx1q2Ef/QJPO4gi6DMKD51xeQ380knDrULcZyIF5vFNWbUvI23PX9LrI
R7oDjKOcd9Y97XehAkmqnUV4r4Gbsk0hkjjRFZ/I7lO2eK8eE2mcSV+TRBMJBPEJEw=="
create_log = function(dir, key, soft_limit, hard_limit)
```

Cadena de texto referenciando a Sauron en el módulo keylogger de Remseck

Finalmente, la firma de soluciones de seguridad ForcePoint reveló los detalles del Grupo del Monzón (Monsoon Group), también conocido como Patchwork AP y Operación Hangover), un equipo de piratas informáticos basados en la India, que ha comprometido cuentas de ciudadanos chinos dentro de diferentes industrias y agencias gubernamentales en el sur de Asia desde el año 2013.

Dropping Elephant

HACKTIVISMO

Tras los ataques del mes de julio a los sistemas informáticos del Comité Nacional Demócrata, a mediados del mes de agosto, *Guccifer 2.0, el hacker que aparentemente participó en la primera fuga de información, filtró un nuevo lote de documentos, notas y contraseñas, esta vez pertenecientes al Comité de Campaña Demócrata del Congreso de EEUU (DCCC).* Incluyen una hoja de cálculo de números telefónicos de contactos en el Congreso y las direcciones de correo electrónico, memorandos internos y lo que podrían ser documentos robados del equipo de Nancy Pelosi, la demócrata de más alto rango en el Congreso.

Finalmente, el grupo hacktivista de *Anonymous atacó diversos sitios web del gobierno brasileño para protestar contra los Juegos Olímpicos en Río de Janeiro bajo la operación #OpOlympicHacking.*

Los objetivos incluyeron:

1. la página web oficial del gobierno federal para los Juegos de 2016 (brasil2016.gov.br)
2. Portal del Gobierno del Estado de Río de Janeiro (rj.gov.br)
3. Ministerio de Deportes (esporte.gov.br)
4. Comité Olímpico de Brasil (COB cob.org.br)
5. Sitio web oficial de los Juegos Olímpicos de 2016 de Río (rio2016.com).

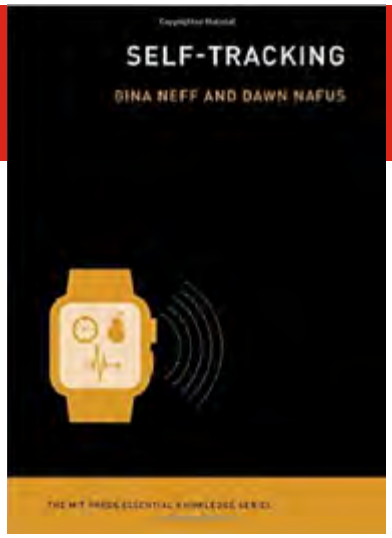
En la segunda fase del ataque, Anonymous Brasil comunicó *la filtración de datos personales del Alcalde de Río de Janeiro, el gobernador de Río de Janeiro, el Ministro de Deportes, el presidente del Comité Olímpico Brasileño y tres hombres de negocios que están presuntamente implicados en casos de corrupción en el país.*

8 Recomendaciones

8.1 Libros y películas

Película:
STAR TREK: MAS ALLA

Sinopsis: El USS Enterprise, la nave insignia de la Flota Estelar liderada por el capitán James T. Kirk, vuelve a surcar el universo para asegurarse de la protección de la Tierra y del resto de planetas aliados. Pero la tranquilidad durará poco y el peligro acecha. La primera etapa de su misión les llevará a un territorio desconocido, y su travesía de vigilancia pronto se convertirá en una carrera por la supervivencia espacial cuando se enfrenten a un nuevo y fiero enemigo, Krall, una especie alienígena avanzada. Para frenar sus siniestros planes, Kirk deberá reunir a su equipo y usar todo sus recursos para resolver los desafíos a los que se enfrentarán. A la vez que intentan encontrar el modo de volver a la Tierra, su misión será proteger el futuro de la raza humana y preservar la armonía entre especies... Tercera entrega de la nueva saga de Star Trek.



Libro:
SELF TRACKING

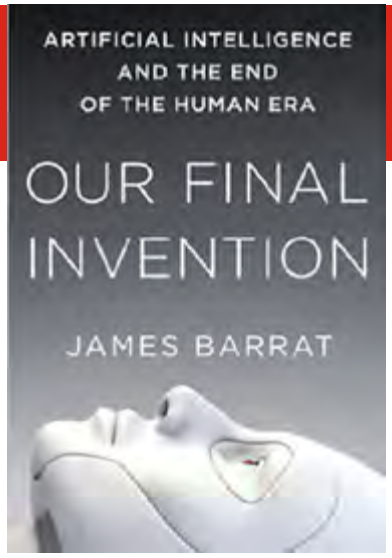
Autor: Gina Neff y Dawn Nafus
Num. Paginas: 248
Editorial: MIT Press
Año: 2016
Precio: 12.50 Euros
Sinopsis: Los autores analizan el fenómeno del ´Self-Tracking´- que consiste en la recolección de datos de todas las actividades que lleva a cabo una persona -seguidora de este fenómeno- a lo largo de su vida cotidiana. Estos datos generan la información necesaria para que estos usuarios optimicen su rendimiento.

Libro:
MOOCS (MIT PRESS ESSENTIAL KNOWLEDGE)

Autor: Jonathan Haber
Num. Paginas: 248
Editorial: MIT Press
Año: 2014
Precio: 11.50 Euros
Sinopsis: Jonathan Haber analiza el fenómeno de los cursos on-line masivos de acceso libre, también conocidos como MOOCs. El autor sostiene que los MOOCs no son la solución a los problemas de la educación mundial pero si facilitan el intercambio de conocimiento y el acceso al mismo por parte de millones de personas.

Libro:
ELECTRONIC DREAMS

Autor: Tom Lean
Num. Paginas: 288
Editorial: Bloomsbury Sigma
Año: 2016
Precio: 11.50 Euros
Sinopsis: Tom Lean nos transporta al universo del ordenador personal en Reino Unido durante la década de 1980. Para ello, el autor ha recabado la opinión de muchos de los protagonistas de la época, entre ellos responsables y usuarios de los míticos ordenadores Amstrad, Sinclair o Acom, entre otros.



Libro:
OUR FINAL INVENTION

Autor: James Barrat
Num. Paginas: 336
Editorial: St Martin´s Griffin
Año: 2015
Precio: 12.50 Euros
Sinopsis: James Barrat proporciona una visión realista, en ocasiones oscura, al más puro estilo Terminator, de las consecuencias que tendrá la popularización de la inteligencia artificial.

8.2 Webs recomendadas

http://www.disa.mil/
Sitio web de la DISA, la Agencia de Sistemas de Informacion y Comunicaciones del Departamento de Defensa de los Estados Unidos.

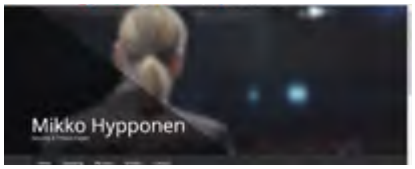
https://www.dhs.gov/science-and-technology
Sitio web del Departamento de Ciencia y Tecnologia del Departamento de Seguridad Nacional de los Estados Unidos.

http://www.enatic.org/
Sitio web de Enatic, grupo de referencia nacional de los Abogados TIC y 2.0.

http://bitactual.es/
Sitio web de BitActual, una revista que cuenta historias sobre el mundo de las TIC con un carácter más periodístico que tecnológico.

http://www.cert.org/
Sitio web del CERT de la Universidad de Carnegie Mellon.

https://mikko.hypponen.com/
Sitio web de Mikko Hypponen, uno de los expertos mas influyentes en el ambito de la seguridad de la informacion.



8.3 Cuentas de Twitter

@cybraryIT

@DSMeu

@UdoEnisa

@IBMSecurity

@NCIAgency

9 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
7-8 sept	Toronto	ICSIC	2016 International Cyber Security & Intelligence Conference	https://icsic.ocmtontario.ca/
8-9 sept	Bruselas	EC, OASIS	BC Borderless Cyber	http://borderlesscyber.oasis-open.org/eu16
8-9 sept	Frankfurt	DG CONNECT, ENISA & Goethe University	Annual Privacy Forum 2016	http://privacyforum.eu/
13-sept	Londres	cityforum	Cyber Security Summit	http://www.cityforum.co.uk/events.asp?eventID=80040
19-20 sept	Londres	The Network Group	Information Security Network	https://thenetwork-group.com/information-security-network/
22-sept	Madrid	IDC	Conferencia sobre Big Data y el valor de la información	http://www.redseguridad.com/eventos/agenda-del-sector/conferencia-sobre-big-data-y-el-valor-de-la-informacion
20-23 sept	La Haya	hardwear.io	hardwear.io Security Conference	http://hardwear.io/
26-27 sept	Cracovia	CYBERSEC & THE KOSCIUSZKO INSTITUTE	CYBERSEC	http://www.cybersecforum.eu/en/
28 sept	Madrid	ISMS Forum	V Foro de la Ciberseguridad	https://www.ismsforum.es/evento/640/v-foro-de-la-ciberseguridad/
29-sep	Madrid	ADSI, AEDS y ASIS International	VI Congreso de Directores de Seguridad Corporativa	http://www.seguritecnia.es/revistas/seg/eventos/VIdirectores2016/VI_congreso_directores_programa.pdf

Patrocinadores

Consejo Asesor Empresarial

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269