DICIEMBRE 2015 / Nº 9

CIBER elcano

Desarrollado por:

INFORME MENSUAL DE CIBERSEGURIDAD

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.

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 17

4 Entrevista a Daniel Barroso 24

5 Informes y análisis sobre ciberseguridad publicados en noviembre de 2015.... 28

6 Herramientas del analista 29

7 Análisis de los ciberataques del mes de noviembre de 2015 31

8 Recomendaciones

8.1 Libros y películas 35

8.2 Webs recomendadas 37

8.3 Cuentas de Twitter.....37

9 Eventos.....38

1 COMENTARIO CIBERELCANO
Responsible Disclosure: el caso holandés

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

Responsible Disclosure. Foto: *ICT Institute.*

Muchos gobiernos y empresas dirigen, gestionan y controlan la defensa de sus ciberespacios específicos desde la eterna crisis y no desde un liderazgo proactivo. Recientemente, la empresa Verizon publicó su *informe anual sobre ciberamenazas*, donde alertaba que el 99,9% de las amenazas cibernéticas están identificadas pero los responsables de seguridad no llevan a cabo ninguna actuación para minimizar este riesgo conocido.

La transición de una **gobernanza del ciberespacio** desde la crisis al liderazgo no es siempre tan evidente ni tan rápida. El caso de los Países Bajos es un claro ejemplo de cómo situaciones de crisis han modificado la manera de gobernar el ciberespacio. En septiembre de 2011, el gobierno intervino *Diginotar* –la autoridad de certificación utilizada por la administración holandesa y la mayoría de las compañías privadas del país y otras multinacionales– tras la falsificación de certificados digitales aparentemente generados por la compañía y utilizados por la CIA, el Mossad o el MI6. Este hecho, unido al hackeo del sistema que controla las chip-cards con las que viajan la mayoría de los usuarios del transporte público del país, situaron a las ***Full Disclosure*** –publicación de vulnerabilidades sin el conocimiento previo del dueño del sistema o proveedor del servicio– en la primera línea de la agenda política holandesa.

A principios de 2013, el gobierno holandés, a través del Centro Nacional de Ciberseguridad (NCSS, por sus siglas en inglés), comienza a trabajar junto a las principales compañías nacionales en la elaboración de una primera

política nacional de *Responsible Disclosure* (tambien conocida como *Coordinated Vulnerability Disclosure*). Esta política tiene como objetivo evitar que las vulnerabilidades sean hechas públicas antes de que el dueño del sistema o proveedor del servicio las conozcan y que posteriormente, y de manera coordinada, éstos y el investigador de seguridad que descubre la vulnerabilidad las puedan hacer públicas si así lo determinan.

Este concepto no es nuevo. Muchas compañías, sobre todo aquellas dedicadas al desarrollo del software, disponen de programas de *Bug bounty* por el cual premian a aquellos investigadores que descubren vulnerabilidades en sus productos. Sin embargo, el éxito de dichos programas es limitado debido a que en muchas ocasiones el "botín" es pequeño (escaso reconocimiento profesional y remuneración económica).

El gobierno holandés *trabajó en el desarrollo* de la política de *Responsible Disclosure* identificando tres actores/roles diferentes: empresa, investigador de seguridad y Equipo de Respuesta para Emergencia Informática o CERT (por sus siglas en inglés) nacional. Para cada uno de estos actores se han definido un conjunto de derechos y deberes que delimitan las "reglas del juego".

Las **empresas** están obligadas a disponer de un grado de madurez mínimo (y suficiente) en materia de ciberseguridad, y gestionar con diligencia aquellas comunicaciones que reciban por parte de los investigadores de seguridad. Los **investigadores de seguridad** no deberán utilizar técnicas de intrusión ilegales, y deberán comunicar de manera responsable a las empresas mediante un estricto procedimiento. Por último, el **CERT nacional** deberá facilitar el contacto entre las empresas y los investigadores de seguridad (sino lo hacen de manera directa), y deberá gestionar los incidentes que afecten a los sistemas Tecnologías de la Información y Comunicación (TIC) de la administración holandesa.

En el caso específico de fallos de seguridad que afectan a sistemas TIC de la administración holandesa, ésta ha puesto a disposición de la comunidad de investigadores de seguridad una dirección de correo electrónico para que estos puedan proporcionar (garantizando la confidencialidad) todos los detalles relativos a los fallos que descubran, así como sus datos personales para poder ser contactados y continuar el proceso de *Responsible Disclosure*. El investigador de seguridad deberá informar de aquellos fallos de seguridad que hayan descubierto de manera legal, y deberá evitar el uso de malware, ataques de fuerza bruta, copiar, borrar o cambiar datos de los sistemas TIC afectados, y compartir información de la vulnerabilidad con terceros. Siempre que el investigador de seguridad realice un *Responsible Disclosure* legalmente, el gobierno estará obligado a investigarla, hacerla pública tras un determinado tiempo, hacer público el nombre del investigador (si así lo desea) y deberá renumerarle en función de la criticidad del fallo descubierto.

En definitiva, el gobierno holandés ha entendido l**a importancia estratégica de los investigadores de seguridad informática para la ciberseguridad nacional.**

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

Diseño de vectores de ataque a través de redes sociales.

AUTORES: Chema García. Analista senior de THIBER.

En la primera década del siglo XXI, comenzaron a popularizarse las denominadas "Redes Sociales Virtuales". En 2003 Microsoft lanzaba MySpace, Mark Zuckeberg creaba Facebook mientras aún estudiaba en la Universidad de Harvard en el 2004, y Jack Dorsey en 2006 crea Twitter Dichas redes eran en sus orígenes, aplicaciones web que permitían construir un perfil público o semi-público dentro de un sistema limitado; articular una lista contactos con otros usuarios con los que comparten una conexión y ver y recorrer su lista de conexiones y actividades así como las realizadas por otros dentro del sistema.

Las redes sociales en internet representan los principales lugares de agregación de datos y usuarios. Millones de usuarios conectados lo utilizan para una amplia variedad de propósitos. El alto nivel de penetración de los medios sociales hace que estas plataformas sean los principales medios para actividades ilegales así como de análisis de inteligencia. En muchos casos, ambos aspectos se unen y se ejercitan de forma similar en la consecución de los mismos objetivos.

El potencial de estas plataformas son enormes y su control, vigilancia y uso son una necesidad creciente en la comunidad de inteligencia.

En este sentido, las agencias de inteligencia de EE.UU., Israel, China y Rusia son los más activas en este campo, pero las autoridades de Irán y Siria han demostrado cierto interés en su monitorización para diferentes propósitos, permitiendo el seguimiento de miles de millones de conversaciones mediante análisis de texto y actividad de usuarios basados en criterios predefinidos.

"... su control, vigilancia y uso son una necesidad creciente en la comunidad de inteligencia."

Las redes sociales comienzan a ser consideradas elementos críticos para actores tanto estatales como no estatales, en el apoyo de operaciones militares, paramilitares e insurgentes, dado que son habilitadores para :

- Operaciones de Información y contra-información (INFOOPS)
- Operaciones psicológicas (PSYOPS)
- Labores de inteligencia de fuentes abiertas (OSINT)
- Espionaje/Contraespionaje
- Actividades ofensivas

Si bien el presente artículo no se centra en el uso de redes sociales para llevar a cabo operaciones psicológicas o para manipular la percepción del adversario, su uso en este sentido a lo largo de los últimos años ha sido exponencial, con casos prácticos tan significativos como la Operación Pilar Defensivo, los movimientos de la Primavera Árabe o el conflicto Sirio y la irrupción del Daesh.

En el documento, "Allied Joint Doctrine for Psychological Operations AJP-3.10.1(A),"," la OTAN ha puesto de manifiesto la posibilidad de apoyar las operaciones militares con Operaciones Psicológicas (PsyOps) buscando los siguientes objetivos básicos:

- Debilitar la voluntad del adversario o adversarios.
- Reforzar el compromiso de los destinatarios aliados.
- Obtener el apoyo y la cooperación de las audiencias no comprometidos o indecisos.

De esta forma, un sujeto podría explotar las redes sociales para desestabilizar una empresa o cualquier otro aspecto de la sociedad moderna. El principal cambio introducido por las PsyOps automatizadas en redes sociales es que todos los actores potencialmente podría controlar la difusión de información sobre los medios de comunicación: los grupos criminales, los contratistas privados de inteligencia, grupos terroristas y hacktivistas podrían influir en el sentimiento global con información artificial con datos convincentes y persuasivos. Este aspecto es fundamental y representa una seria amenaza para la sociedad contemporánea de la información.

Es por esto que, la *Agencia de Proyectos Avanzados de Investigación de Defensa (DARPA)*, parte integral del Departamento de Defensa norteamericano (DoD), ha desarrollado un programa específico *de Comunicación Estratégica en Medios de Comunicación Social (SMISC)*. A través de este programa, DARPA busca desarrollar herramientas para apoyar los esfuerzos de los operadores humanos para contrarrestar la desinformación o campañas de engaño con información veraz, detectando cualquier acción inducida por agentes externos a dar forma el sentimiento global o de opinión en la información generada y se extendió a través de los medios sociales.

A fin de lograr dichos objetivos, el programa SMISC se centra en la investigación de claves lingüísticas, análisis de patrones de flujo de información y detección de sentimientos u opiniones sobre la información generada y extendida a través de redes sociales. Los investigadores del programa exploran ideas y conceptos para analizar los patrones narrativos y culturales. El éxito del SMISC depende la capacidad para modelar las comunidades emergentes y analizar el flujo de información y sus participantes , así como caracterizar la generación de contenido automatizado por redes de bots, en los medios sociales.

Por otra parte, entre las actividades de DARPA se ha incluido el estudio la manera de pronosticar el comportamiento dinámico grupos de usuarios en las redes sociales –conocido como forecasting grupal en redes sociales-. A pesar de que el uso de las redes sociales ha sido ampliamente investigado, poca atención se ha prestado a cómo los grupos de influencia (por ejemplo paramilitares o grupos yihadistas) compiten entre sí por la captación miembros y su influencia en las opiniones de los otros equipos y comunidades. "Es necesario comprender lo afecta este comportamiento en línea de predicción de tendencias."

"…el análisis de redes sociales es un poderoso apoyo para las operaciones de inteligencia…"

Queda claro que el análisis de redes sociales es un poderoso apoyo para las operaciones de inteligencia en particular debido a que su análisis permite llevar a cabo operaciones de inteligencia de fuente abierta OSINT para obtener información. Su aplicación militar, por ejemplo, permitiría la recolección de información de dominio público sobre objetivos estratégicos.

En el ámbito del DoD norteamericano se están abordando proyectos de desarrollo de conceptos y experimentación a través de la definición de una nueva generación de instrumentos que podrían utilizarse para el análisis masivo en tiempo real de información en redes sociales con la intención específica de proporcionar alerta temprana sobre situaciones de interés. En este sentido, ***se ha creado un portal web dedicado*** a proporcionar cualquier tipo de información relacionada con el uso de los medios sociales en el ámbito militar y, más en general, para los ciudadanos que desean entender mejor estas plataformas. El sitio web está diseñado para ayudar a la comunidad del Departamento de Defensa a usar los medios sociales y otras funciones basadas en Internet (IbC) de manera responsable y eficaz, dificultando las labores OSINT a potenciales adversarios.

Sin embargo, existen obstáculos a las actividades OSINT en redes sociales, como las restricciones nativas de dichas plataformas aplicadas para preservar la privacidad de los usuarios. Asimismo, el éxito de un programa OSINT basado en el análisis de redes sociales de los siguientes habilitadores:

- Dimensión de los datos adquiridos.
- Capacidad de correlacionar de forma correcta la información.
- Evitar el "envenenamiento" de información, ya sea intencionado o involuntario, ya que su inclusión en el análisis conllevaría conclusiones erróneas, causando la pérdida de consistencia en los resultados.
- Dinamismo de los usuarios las redes sociales, un mismo individuo por lo general emplear diferentes perfiles en redes diversas, complicando el mero análisis comparativo.

El análisis de toda esa información de forma agregada y correlada, empleando técnicas de minería de datos y *big data analysis*, supone el establecimiento de una base clara de operaciones de análisis de señales (SIGINT) a través de información de libre acceso o pública (OSINT).

¿Y LA SEGURIDAD EN LAS REDES SOCIALES?

A raíz del auge de las redes sociales mencionadas, numerosos investigadores de seguridad (tanto investigadores individuales, como grupos de estudio empresariales) algunos con más ética que otros, centran su atención en la búsqueda de puntos débiles en el sistema que les permitiese en mayor o menor medida aprovecharse de la gran afluencia de usuarios hacia este tipo de portales; Y es que, si hasta hace relativamente poco, los ataques en masa se realizaban contra organizaciones y empresas, cada vez existen más actores que se centran única y exclusivamente en atacar el eslabón más débil: el usuario final.

Las redes sociales se han convertido en un ecosistema excelente para diversos tipos de malware, principalmente porque permiten difundir dichos códigos maliciosos a un público amplio que, por lo general, tienen poco conocimiento de principales amenazas cibernéticas.

El uso de las redes sociales podría permitir a los atacantes reclutar un gran número de "zombies" (ordenadores infectados) para llevar a cabo una ofensiva exitosa contra blancos críticos (por ejemplo, infraestructuras críticas o gubernamentales) y/o obtener beneficio económico. Otra de las ventajas en la explotación de plataformas de medios sociales es la posibilidad de dirigirse a grupos de individuos de una comunidad seleccionada que comparten actitudes y hábitos particulares , por lo general con fines de espionaje.

En el último par de años, ha proliferado el malware diseñado específicamente para propagarse a través de las redes sociales, permitiendo ataques a gran escala , así como ataques APT, y también para ocultar la infraestructura de comando y control y su el tráfico relacionado.

El motivo principal que suele llevar a determinados colectivos a atacar a los usuarios, suele ser para, una vez comprometido el sistema, obtener sus credenciales de acceso a distintos portales Web (Banca online, redes sociales, email, etc.), utilizarlos como puentes para otros ataques, utilizar su capacidad de computación, datos, etc. Y es en este punto donde entran las redes sociales, en este caso concreto: Twitter.

¿POR QUÉ TWITTER?

Una de las características principales de esta red social, es la posibilidad de crear y usar "hashtags" [1], para categorizar un mensaje sobre el que cualquier usuario puede hacer un aporte u opinión personal con solo escribir dicho "hashtag" en el mensaje. Esta característica permite buscar mensajes categorizados en tiempo real y enlaces a contenidos en función de una temática concreta (los más usados por los usuarios son los llamados "Trending Topics"), y lo más relevante de cara a un marco OSINT, cualquier usuario puede enviar un mensaje con un "hashtag" determinado, de manera que dicho mensaje esté disponible para cualquier usuario que consulte los mensajes en el timeline de dicho "hashtag".

Adicionalmente debido a la restricción de los 140 caracteres permitidos en los mensajes, se hizo popular el uso de acortadores de URLs (como bit.ly o t.co entre otros muchos), y aunque el uso de estos acortadores de URLs es un riesgo conocido, siguen siendo ampliamente usados.

"...320 Millones de usuarios en todo el mundo y 400 millones de tweets al día..."

Con cerca de 320 Millones de usuarios en todo el mundo y 400 millones de tweets al día, Twitter representa una fuente extraordinaria para la clasificación y localización de perfiles así como para tareas OSINT, dadas las siguientes características:

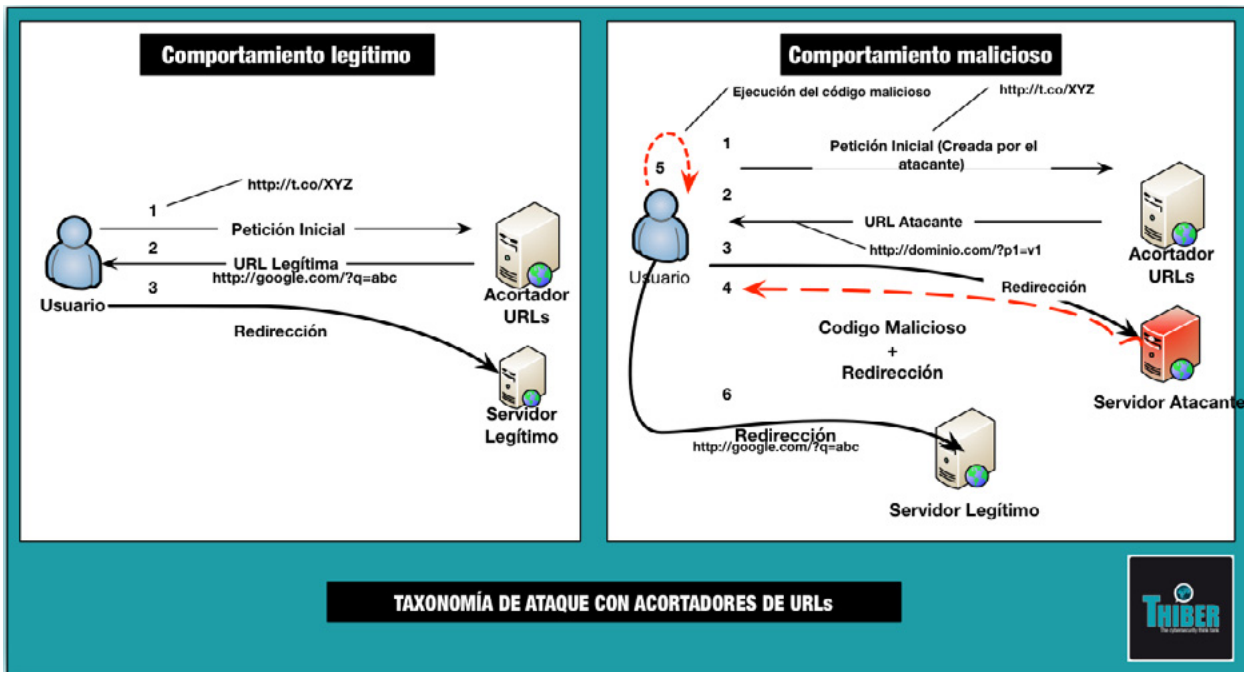
- Búsquedas en tiempo real
- Detección de tendencias de forma automática, basado en algoritmos complementarios como el conteo simple, los test chi-cuadrados o modelos específicos de tendencias.
- Interesante información ofrecida por la plataforma, como geolocalización, idioma de publicación, velocidad de publicación de tweets o el grado de influencia.

LA INSEGURIDAD DE LOS ACORTADORES DE URL

El acortamiento de URL es una técnica web en la que longitud de una URL se vincula a una URL significativamente más corta pero manteniendo el enlace directamente a la página original.

Estos acortadores son potencialmente peligrosos debido a que se basan en la confianza del usuario, ya que el usuario no sabe qué contenido será cargado en el momento en el que navega por esa URL, o qué se cargará antes de enviarnos a la URL legítima. El vector de ataque más habitual ante este tipo de tecnologías consiste en enviar a un usuario a una Web controlada (puede ser maliciosa o inocua), que permita enviar al navegador del usuario un "objeto" que será interpretado/ejecutado en su navegador. Estos "objetos" suelen ser Java Scripts, Flash, PDF y Applets Java, debido a que se ejecutan en el propio navegador del cliente, permitiendo explotar vulnerabilidades (existentes en sistemas no actualizados, o 0days) y tomar el control del equipo y/o navegador del usuario, ataque conocido como "Drive-by Exploits", que constituye el vector de ataque más común actualmente según el último informe de amenazas de ENISA [13].

La web intermedia bajo el control del atacante puede ser una creada específicamente para este fin, o bien ser una web comprometida en la que se pueda modificar su contenido para que el usuario cargue el contenido malicioso específico.



Taxonomía de ataque con acortadores de URL

Twitter ofrece un gran potencial ante este vector de ataque, ya que cada vez que se publica un mensaje con una URL, ésta es automáticamente acortada, lo que hace que los usuarios se encuentren familiarizados con este tipo de URLs y no duden en visitar dicho enlace; Más aún si creen que dicho enlace proviene de una fuente conocida o el contenido mostrado es legítimo.

Llegados a este punto, se hace evidente que a grandes rasgos y sin entrar en detalles técnicos, es factible comprometer el sistema de un usuario haciendo que visite un enlace publicado en un "Tweet", si el contexto le resulta interesante o conocido.

Y es aquí donde intervienen los "Hashtags" mencionados anteriormente, y es que los propios usuarios se están auto-clasificando en colectivos mediante el uso de dichos "categorizadores", y lo que es mejor, la propia red social nos permite obtener un listado con todos los mensajes y todos los usuarios ordenados por *posición geográfica y temática.* Si a eso le sumamos herramientas de monitorización que incluso nos permiten conocer visualmente sobre un mapa los "Trending Topic" y "Hashtags" en tiempo real [9][10][11][14], tenemos la posibilidad de realizar ataques dirigidos sobre grupos concretos de personas según sus intereses y posición geográfica, con un coste realmente bajo.

ACCESO DE LOS USUARIOS A LA RED Y A TWITTER

Según varios informes actuales [2][3][5][7] se está atravesando un incremento en el acceso a internet a través de dispositivos móviles (el **82%** de los usuarios acceden a través de estos dispositivos), y concretamente el acceso a redes sociales. Tanto es así, que Twitter ha duplicado sus usuarios registrados de 2010 a 2011 teniendo un 63% de los usuarios activos, el 36% y el 51% de los usuarios

que abandonan redes sociales como Tuenti o Google+ respectivamente, se registran en Twitter, siendo un 61% hombres con una media de edad de 28,30 años (el 56% tiene más de 25 años).

De entre todos estos usuarios, los que acceden a través de dispositivos móviles lo hacen o bien a diario (42%) o al menos una vez al mes (52%).

Atendiendo a otros informes [4][6] el uso de antivirus en estos terminales (aunque ha sufrido un incremento) se sitúa en el **10,7%**, Se espera que el número de dispositivos móviles con conexión a internet aumente debido a su alta demanda.

MARCO DEL EJERCICIO

Taxonomía del Ataque

El vector de ataque que se plantea se desenvuelve en un entorno multicapa. Si bien el uso de las redes sociales para la obtención de información o la difusión de malware no es un concepto nuevo, el uso de Twitter para realizar tareas de localización de objetivos y OSINT y atacantes podrían utilizarlo para adquirir una gran cantidad de información personal sobre los objetivos, los medios de comunicación social es ideal para operaciones de inteligencia/contrainteligencia a largo plazo.

Por todo ello, se realiza una aproximación combinando múltiples debilidades que permitiría el descubrimiento, revelación, destrucción de información:

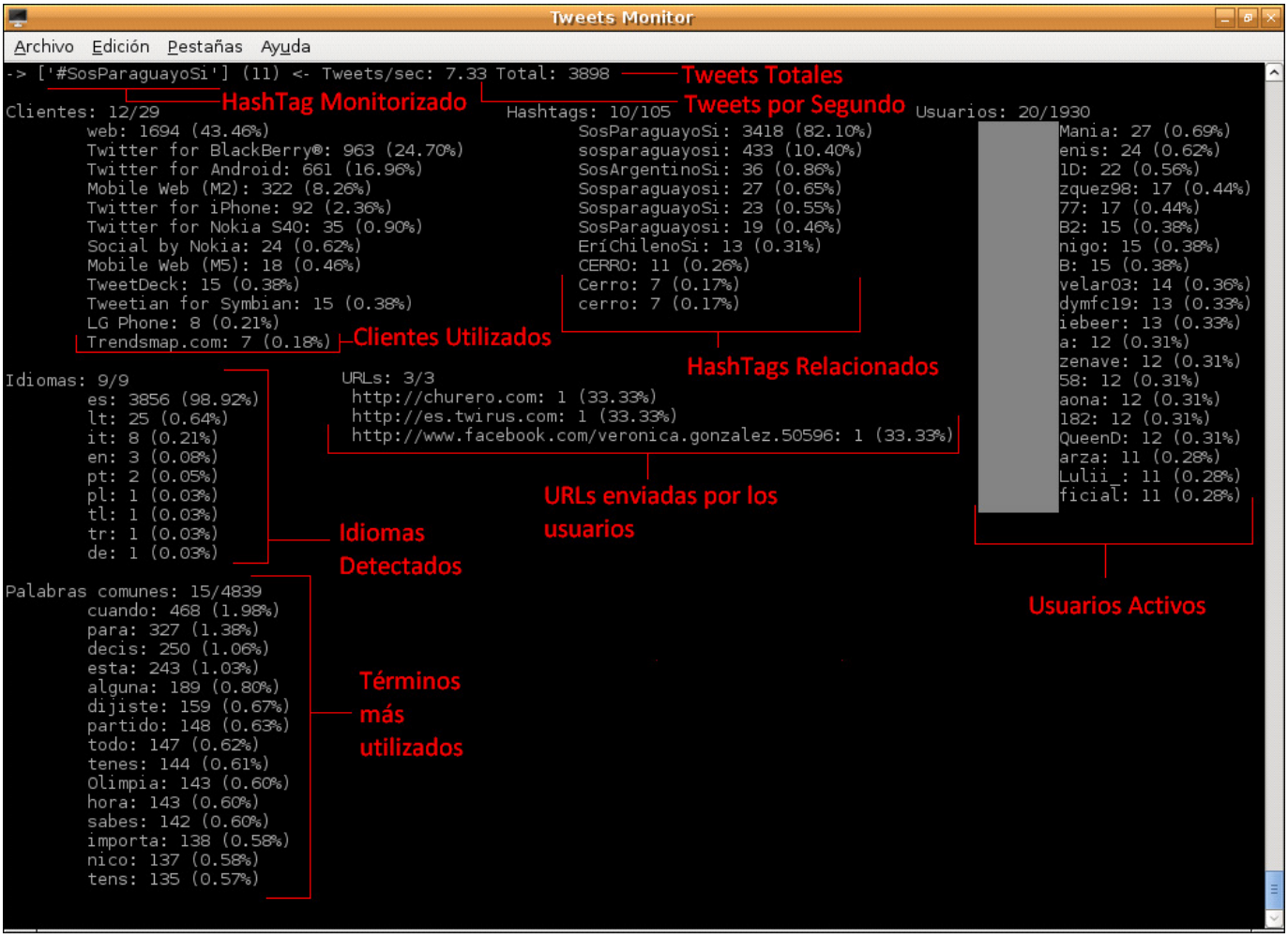
- Monitorización pasiva de redes sociales
- Selección de objetivos
- Elaboración de mensajes atractivos y de “perfil bajo”.
- Ingeniería Social para la distribución de enlaces maliciosos a través de servicios de acortadores de URLs.
- Fallos de seguridad en dispositivos móviles.

Desde una visión más amplia, el ataque estaría dividido en al menos, dos fases:

- **Fase 1 – Focalización**
- Recolección
- Análisis y validación de información
- Estudio y perfilado de objetivos

- **Fase 2 - Materialización**
- Materialización del ataque contra los objetivos estudiados.
- Ejecución del objeto del ataque

Para conseguir lo expuesto anteriormente, se fijan como objetivos nominales los usuarios o grupos de usuarios, las aplicaciones a emplear y los dispositivos móviles de los usuarios/ colectivos objetivo, requiriendo una mínima intervención por parte del atacante, ya que esta fase puede ser realizada por aplicaciones automatizadas y sistemas especialmente diseñados para esta tarea.



Monitorización de HashTags

La Fase 2 del ataque, puede ser originada desde:

- Perfiles de Confianza: Perfiles que generan cierto nivel de confianza en el objetivo, bien sea porque el objetivo conoce/es seguidor del perfil en cuestión, por ser un perfil conocido públicamente, un perfil oficial (acreditado por Twitter), etc.

- Perfiles Externos: Perfiles desconocidos por el objetivo en los que no existe relación de confianza.

Para materializar la Fase 2 usando Perfiles de Confianza, podrían darse los siguientes escenarios:

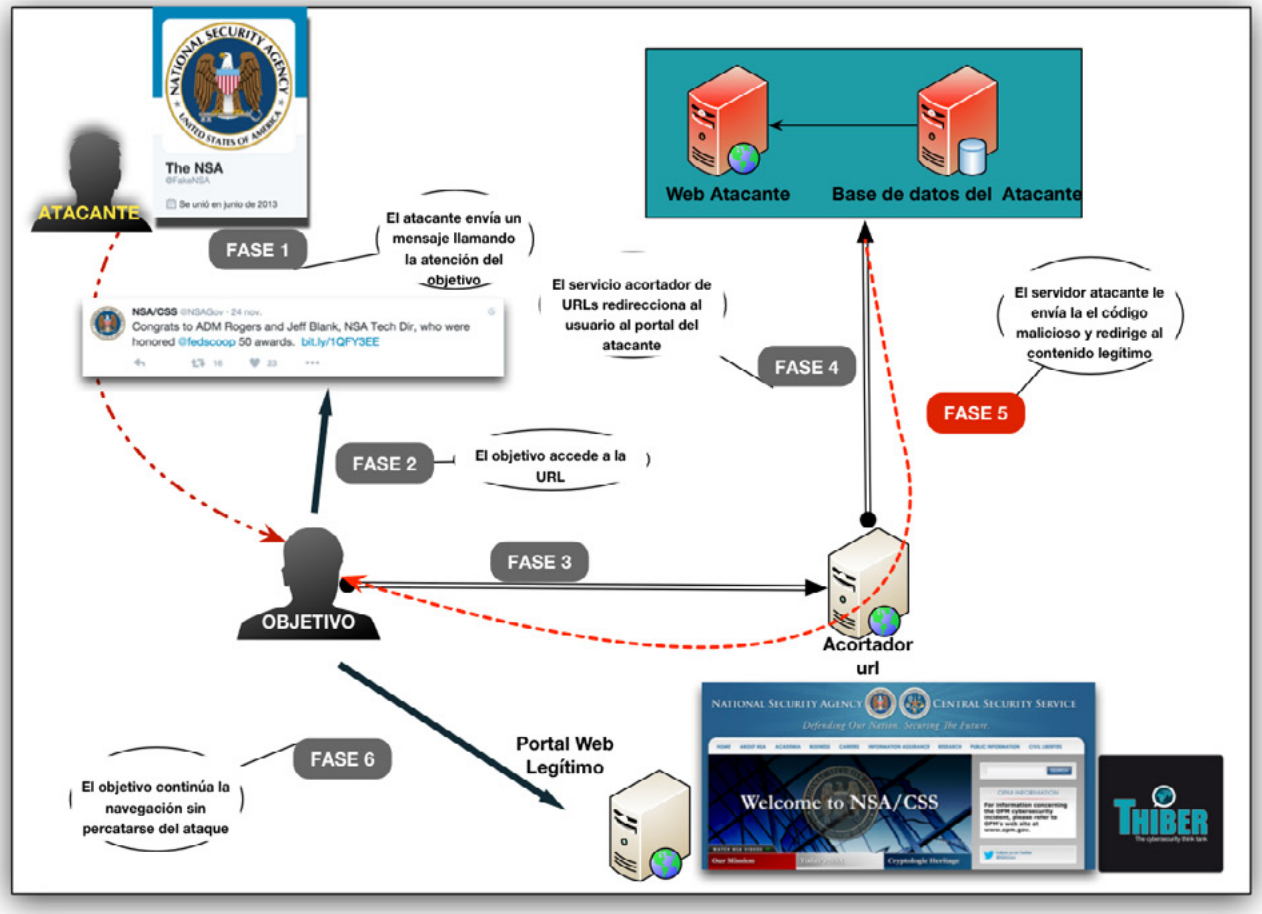
- El atacante aprovecha la relación de confianza (por cuenta propia).
- Un tercer atacante (Atacante0) "fuerza" al atacante (Perfil de Confianza con el objetivo) a explotar la relación de confianza.
- Perfil de Confianza comprometido, se usa como atacante para hacer uso de la relación de confianza con el resto de usuarios.
- Perfil falso simulando un perfil legítimo.
  - Inconveniente: Número de seguidores
  - Solución: Incrementar el número de seguidores
    - Cuentas comprometidas
    - Fallo en la aplicación Web (XSS/ CSRF)
    - Bots
  - Inconveniente: Número de Tweets
  - Solución: Clonado del TimeLine del perfil legítimo

Escenarios posibles usando Perfiles Externos:

- Mensaje con mención al objetivo
- Mensaje (con o sin mención), auto-clasificado usando hashtags
- Mensaje a un "debate" (clasificado según hashtags) es "re-twiteado" por el perfil "moderador".

En mayor o menor medida, es necesario crear un mensaje acorde a la información obtenida en la Fase 1 sobre el objetivo, para llamar su atención.

A continuación, se muestra un gráfico explicativo de la materialización de la Fase 2 del ataque usando el 4º escenario:



Descripción de la Fase 2 del ataque (Perfil de origen falso)

En base a lo anterior, se ha realizado una prueba de concepto compuesta por el siguiente sistema:

- Sistema pasivo de monitorización de "Hashtags"
- Sistema pasivo de recolección de información de clientes

Aunque los dos sistemas mencionados anteriormente realizan sus funciones de forma pasiva de manera que no resulte intrusivo en ningún momento para el/los usuario/s, para el sistema de recolección de información de los usuarios, se requiere el envío de la URL y la interacción por parte del mismo.

No obstante, se ha procedido a realizar una prueba de concepto con una ventana temporal bastante reducida (Nota: Las siguientes imágenes no se corresponden entre sí).

La siguiente imagen muestra algunos datos de usuarios recopilados durante la ventana temporal de la prueba:

+ Options

					id	ip	fecha	visitas
Edit	Inline Edit	Copy	Delete		29	[redacted].53	2013-[redacted]:16:14	2
Edit	Inline Edit	Copy	Delete		30	[redacted].51	2013-[redacted]:16:28	1
Edit	Inline Edit	Copy	Delete		32	[redacted].59	2013-[redacted]:16:56	2
Edit	Inline Edit	Copy	Delete		33	[redacted].56	2013-[redacted]:17:03	15
Edit	Inline Edit	Copy	Delete		48	[redacted].63	2013-[redacted]:17:16	1
Edit	Inline Edit	Copy	Delete		50	[redacted].67	2013-[redacted]:17:30	1
Edit	Inline Edit	Copy	Delete		51	[redacted].64	2013-[redacted]:17:44	1
Edit	Inline Edit	Copy	Delete		52	[redacted].85	2013-[redacted]:17:54	3
Edit	Inline Edit	Copy	Delete		54	[redacted].65	2013-[redacted]:18:09	2

Extracto de visitas e IPs

+ Options

					peticion	nombre	descripcion
Edit	Inline Edit	Copy	Delete		32	Google Earth Plugin	GEPlugin
Edit	Inline Edit	Copy	Delete		32	VLC Web Plugin	VLC media player Web Plugin 2.0.0
Edit	Inline Edit	Copy	Delete		33	Java(TM) Platform SE 7 U11	Next Generation Java Plug-in 10.11.2 for Mozilla b...
Edit	Inline Edit	Copy	Delete		33	QuickTime Plug-in 7.7.3	The QuickTime Plugin allows you to view a wide var...
Edit	Inline Edit	Copy	Delete		33	ActiveTouch General Plugin Container	ActiveTouch General Plugin Container Version 105
Edit	Inline Edit	Copy	Delete		33	NVIDIA 3D Vision	NVIDIA 3D Vision plugin for Mozilla browsers
Edit	Inline Edit	Copy	Delete		33	NVIDIA 3D VISION	NVIDIA 3D Vision Streaming plugin for Mozilla brow...
Edit	Inline Edit	Copy	Delete		33	iTunes Application Detector	iTunes Detector Plug-in
Edit	Inline Edit	Copy	Delete		33	Adobe Acrobat	Adobe PDF Plug-In For Firefox and Netscape 10.1.4
Edit	Inline Edit	Copy	Delete		33	Silverlight Plug-In	5.1.10411.0
Edit	Inline Edit	Copy	Delete		33	IntelÂ® Identity Protection Technology	Intel web components updater - Installs and update...
Edit	Inline Edit	Copy	Delete		33	IntelÂ® Identity Protection Technology	Intel web components for IntelÂ® Identity Protecti...
Edit	Inline Edit	Copy	Delete		33	Windows LiveÂ™ Photo Gallery	NPWLPG
Edit	Inline Edit	Copy	Delete		48	DivX Plus Web Player	DivX Plus Web Player version 2.2.0.52
Edit	Inline Edit	Copy	Delete		50	Java Deployment Toolkit 6.0.180.7	NPRuntime Script Plug-in Library for Java(TM) Depl...

Extracto de plugins detectados

CONCLUSIONES

La minería de datos en redes sociales es una actividad frecuentemente realizada por un número cada vez mayor de actores estatales (agencias de Inteligencia, FCSE, militares, etc.) pero también por parte de actores no estatales como cibercriminales y grupos terroristas con unos fines muy claros:

- Perfilado de usuarios
- Localización de objetivos
- Análisis de relación entre sujetos
- Relaciones entre subconjuntos de información

REFERENCIAS

- [1] *¿Qué son las Etiquetas (Símbolos "#")? .*
- [2] *Los dispositivos móviles comienzan a ser el medio más habitual para acceder a Internet.*
- 3] *El acceso a internet a través de dispositivos móviles crece un 82%.*
- [4] *Estudio sobre seguridad en dispositivos móviles y smartphones, informe anual 2011.*
- [5] *Los smartphones se consolidan como vía de acceso las Redes Sociales.*
- [6] *Estudio sobre seguridad en dispositivos móviles y smartphones (1er cuatrimestre 2012).*
- [7] *Informe de resultados Observatorio Redes Sociales*
- [8] *Atento a las estafas que circulan por las redes sociales.*
- [9] *Organizing the Worl's Hashtags.*
- [10] *Real-Time local Twitter Trends.*
- [11] *Twitter Trends on a Map, worldwide*.
- 12] *Geolocation analysis of Twitter accounts and tweets.*
- [13] *ENISA Threat Landscape.*
- [14] *Social Media Monitoring Tools.*
- [15] *An exhaustive Study of Twitter Users Across de Worl.*
- [16] *Las redes sociales como herramienta de comunicación estratégica de las Fuerzas de Defensa de Israel durante la operación Pilar Defensivo en Gaza.*
- Clarke, R. A., Knake R. K. Guerra en la Red. Los Nuevos Campos de Batalla, Barcelona, Ariel, 2011, p. 296

3 OPINIÓN CIBERELCANO
Smart cities como unidad básica de ciberseguridad

AUTOR: Beatriz Serrano Casas . Especialista en relaciones internacionales y editora en *diplomacydata.com*.

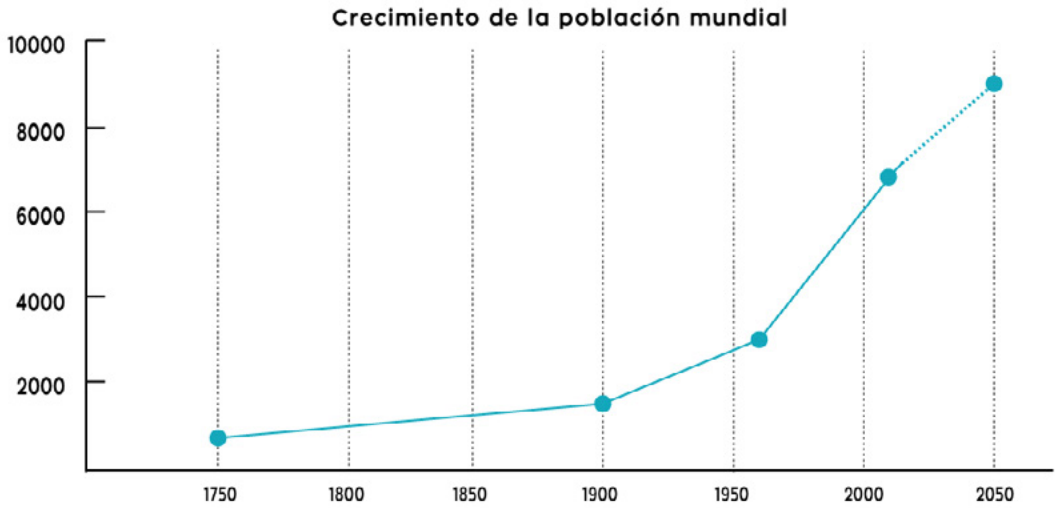
Las relaciones internacionales se han ocupado, desde su nacimiento como disciplina, de las relaciones entre estados. El tratado de Westfalia, firmado en 1648, marcó la supremacía del Estado como unidad en el tablero mundial. Sin embargo, a lo largo de la historia son muchos los actores supra y sub-estatales que han marcado hitos a escala internacional, desde la ciudad babilonia, la polis griega y la ciudad estado veneciana, hasta las organizaciones internacionales nacidas a partir de la Segunda Guerra Mundial.

El carácter multipolar, cambiante y disruptivo del panorama global ha provocado que destaquen en la escena internacional nuevos actores. Un ejemplo son las ciudades que, en ciertos campos, están cobrando más importancia que el propio Estado. Destaca el papel de la ciudad como centro de innovación y punto de partida estratégico para numerosas cuestiones como el desarrollo, el medio ambiente, la diplomacia y la seguridad.

Uno de los campos que hace más relevante el papel de la ciudad es la ciberseguridad. Con una población mundial crecientemente urbana y un suministro de bienes y servicios que tiende a estar cada vez más interconectado utilizando las TIC, al tiempo que las amenazas también son más globales, sofisticadas y complejas tecnológicamente, es vital definir la ciudad como unidad básica para la defensa y resiliencia.

CRECIMIENTO DE LA POBLACIÓN URBANA

David J. Kilcullen, en su artículo "La ciudad como un sistema: el conflicto futuro y la resiliencia urbana", destaca que, al comienzo de la revolución industrial (1750), la población mundial era de 700 millones y en 2009 la cifra era ya de 7.000 millones (ver gráfico). En 1800 sólo un 3% de la gente vivía en una ciudad de al menos un millón de personas. En 2008 por primera vez se pasó el hito del 50% de urbanización de la población.



Fuente: Elaboración propia, datos David J. Kilcullen

En *"Cómo las ciudades están dando forma a las relaciones internacionales"*, Juliana Kerr afirma que Naciones Unidas estima que en 2050, dos tercios de la población mundial vivirán en ciudades. Según el Instituto Global de McKinsey, en los próximos diez años, 600 ciudades sumarán alrededor del 65% del crecimiento global del PIB. Y el mercado para las ciudades inteligentes, se estima que alcanzará los 408.000 millones en 2020, según recoge el informe de Tom Saunders y Peter Baeck para Nesta, Intel y UNDP *"Repensando las smart cities desde la base"*. En palabras de la ex secretaria de estado de EE.UU. Madeleine Albright, "necesitamos entender mejor las dinámicas entre las ciudades globales del futuro y los estados-nación para afrontar los retos del siglo XXI", nos recuerda Kerr.

LA CIUDAD INTELIGENTE O *SMART CITY*

En general, se denomina *smart city* o ciudad inteligente a una en la que los servicios están interconectados y racionalmente optimizados, a través de la tecnología y las redes, para mejorar la calidad de vida de sus habitantes de forma sostenible.

El *"Smart Cities Group"* del MIT concibe la ciudad como "sistema de sistemas" con "oportunidades emergentes para introducir sistemas nerviosos digitales, capacidad de respuesta inteligente y optimización a todos los niveles de integración, desde el de los dispositivos y aplicaciones individuales (…) al de los edificios y, en última instancia, al de ciudades enteras y regiones urbanas".

Symantec define *smart city* como el "suministro inteligente de servicios que se sirve de las tecnologías de comunicación e información como facilitador fundamental, donde los sistemas implicados pueden beneficiarse de la habilidad de estar altamente conectados a través de varias tecnologías". Según la empresa de software de seguridad, hay varios servicios en los que el suministro inteligente será especialmente relevante:

Principales servicios inteligentes en las smart cities

SERVICIOS	APLICACIÓN
Energía y redes de distribución	60 - 80% de la energía mundial se consume en ciudades, es vital optimización de suministro y consumo.
Transporte y movilidad	Impacto en seguridad pública, medioambiente, energía, servicios de urgencias y negocios. Sistemas de control centralizados reciben datos de GPS, comunicación M2M y tecnologías wifi y RFID.
Asistencia sanitaria	Telemedicina, sensores y dispositivos de tratamiento de pacientes e historial electrónico del paciente disponible para los servicios médicos.
Seguridad pública	Televigilancia, protección contra el crimen y el terrorismo y respuesta ante accidentes o catástrofes, mediante intercambio de información y tratamiento de datos en tiempo real.
Comunicación	Sin cables en todos los sectores de la actividad urbana, con oferta de cobertura inalámbrica por parte de actores relevantes.
Urbanismo y vivienda	Ciudad inteligente como conjunto de unidades compactas, "ciudad celular" (MIT), resiliente y autosuficiente y conectada a una infraestructura urbana mayor.

Fuente: Elaboración propia, a partir de Symantec y MIT

Resulta evidente que el concepto de ciudad inteligente está ligado a otros dos conceptos fundamentales para que ésta funcione y se considere como tal:

· Internet de las Cosas (IoT), entendido como cantidad masiva de dispositivos (se calcula que en 2020 serán más de 50.000 millones) interaccionando con unidades de control a través de sensores, RFID, M2M, satélite y GPS.

· *Big data*, debido a la cantidad de datos que generan todos los sistemas, y que requieren una gran capacidad de almacenamiento, análisis, gestión y protección.

Otra clasificación es la de la *Asociación Europea de Innovación de Smart Cities y Comunidades (EIP-SCC)*, que señala seis categorías de acción para potenciar la innovación y competitividad y mejorar la calidad de vida en ciudades inteligentes:

· Procesos e infraestructuras integradas.
· Movilidad urbana sostenible.
· Distritos y medio construido sostenibles.
· Enfoque en el ciudadano.
· Modelos de negocio, finanzas y compras.
· Política y regulación y planificación integrada.

PRINCIPALES AMENAZAS Y VULNERABILIDADES A LAS QUE SE ENFRENTA UNA *SMART CITY*

Las principales amenazas a las que se enfrenta una ciudad inteligente son ataques online a los dispositivos que proporcionan los servicios antes mencionados. Según Microsoft, las amenazas y vulnerabilidades pueden dividirse en pasivas o activas, según la siguiente clasificación:

Amenazas y vulnerabilidades a la ciberseguridad de la smart city

AMENAZAS	EJEMPLOS
PASIVAS	
Acciones involuntarias	Exposición a malware por email o web Recepción de email de spam o phishing
Infradotación recursos	Sistemas desprotegidos Estrategias de mitigación confusas Capacidades de respuesta no definidas Falta de responsabilidad clara
ACTIVAS	
Cibercrimen	Fraude y estafa DDoS Malware y spam Tácticas de phishing Botnets Robo financiero o propiedad intelectual Abuso o daño de sistemas TIC Daño a infraestructuras críticas
Amenazas naturales	Tifones y huracanes Terremotos y tsunamis Inundaciones Corte accidental de cables submarinos

Fuente: Elaboración propia, a partir de Microsoft

Estas amenazas y vulnerabilidades de las ciudades hacen prioritario el desarrollo de resiliencia. En *"Ciber-resiliencia"*, del Instituto Español de Estudios Estratégicos, Luis de Salvador Carrasco explica cómo "la resiliencia es una cualidad inherente a un organismo, entidad, empresa o estado que le permite hacer frente a una crisis sin que su actividad se vea afectada". Además, requiere una estrategia a largo plazo e integral, porque implica todos los niveles de seguridad. Destaca la ciberresiliencia como principio de seguridad recogida en la *Estrategia de Ciberseguridad de la Unión Europea* como prioridad y objetivo a alcanzar, por delante de otros que podrían parecer más relevantes a corto plazo.

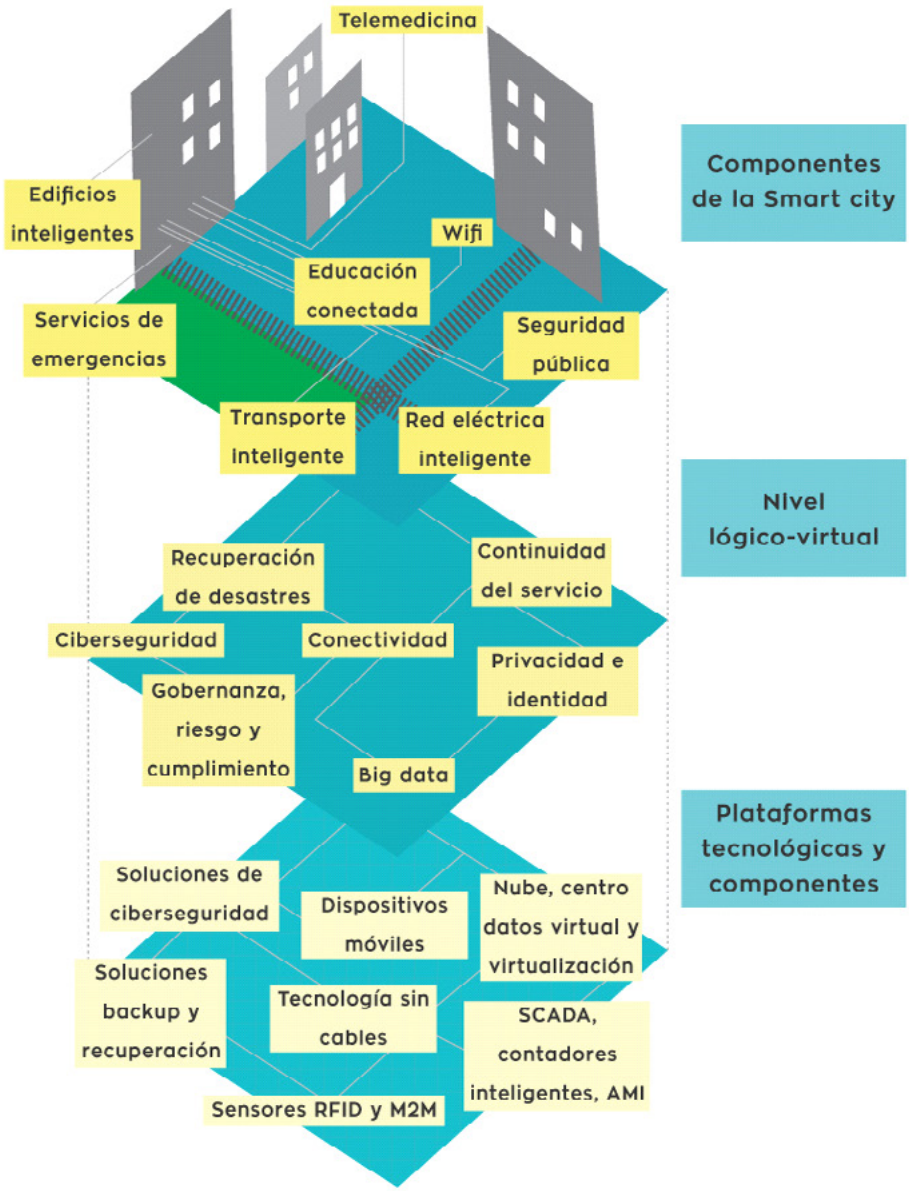
CIBERSEGURIDAD EN LA CIUDAD INTELIGENTE

Todo esto muestra el gran reto al que se enfrenta la ciudad inteligente en cuanto al suministro de servicios, funcionamiento de las redes e integración de sistemas de forma eficiente y sostenible. Por ello es necesario contar con un gran sistema de ciberseguridad adecuado a las características de la *smart city* y las amenazas y vulnerabilidades a las que está sometida.

Para entender la integración de la ciberseguridad en la ciudad inteligente, Symantec describe la *smart city* en tres niveles:

- El nivel superficial, con los componentes de la *smart city* como edificios inteligentes, telemedicina y asistencia médica conectada, seguridad pública, educación conectada y aprendizaje a distancia, transporte inteligente y automotriz, red eléctrica inteligente, servicios de emergencia y puntos wifi gratuitos.
- El nivel intermedio sería el nivel lógico y virtual, correspondiente a los protocolos, medidas y ejes de acción que entran en juego en la ciudad inteligente: ciberseguridad de las ciudades, recuperación de desastres, continuidad del servicio, gobernanza, riesgo y cumplimiento de estándares, conectividad, *big data*, y privacidad e identidad.
- El nivel más profundo se trataría de plataformas y componentes tecnológicos necesarios para el funcionamiento adecuado de la ciudad: soluciones de ciberseguridad, soluciones de backup y recuperación, Sensores RFID y M2M, tecnología sin cables, dispositivos móviles, nube (híbrida, privada o pública), centro de datos virtual y virtualización, SCADA (Supervisión, Control y Adquisición de Datos), contadores inteligentes y AMI (Infraestructura de Medición Avanzada).

Niveles de integración de la ciberseguridad en la smart city



Fuente: Elaboración propia, a partir de Symantec

Según todo lo anterior, Microsoft define la ciberseguridad de una ciudad inteligente como la "protección de datos, sistemas e infraestructura vital para el funcionamiento de la ciudad y para la estabilidad y subsistencia de sus habitantes".

SOLUCIONES Y RECOMENDACIONES DE CIBERSEGURIDAD PARA LA *SMART CITY*

Para construir una estrategia de ciberseguridad y realizar con éxito la transición a una *smart city* segura, los expertos realizan varias recomendaciones:

- Establecer un marco de trabajo de gobernanza. Como afirman Félix Arteaga y Enrique Fojón Chamorro en su *comentario en el Real Instituto Elcano*, la gobernanza es crítica como base para la estrategia de ciberseguridad donde se haya identificado y se implique a las partes afectadas más relevantes en los distintos niveles y sectores: administración local y estatal, industrias, sector privado y universidad. Es fundamental pasar a un modelo de gobernanza "de política pública de mayor recorrido y más largo plazo".

- Utilizar como punto de partida una adecuada evaluación y gestión de riesgos. Para ello, hay que valorar las amenazas a la ciberseguridad, teniendo en cuenta el nivel aceptable de exposición al riesgo, realizando una evaluación continua en el tiempo y definiendo roles y responsabilidades.

- Establecer prioridades claras para proteger las infraestructuras críticas cuyo deterioro podría afectar gravemente al funcionamiento de la ciudad y garantizar la disponibilidad continua de aquellas cuyo funcionamiento ininterrumpido es esencial para la ciudad inteligente. Es clave establecer un sistema que permita equilibrar suministro tradicional y de nube para minimizar la exposición a los riesgos e implantar sistemas fuertes de autentificación de los usuarios que minimicen la exposición a intrusiones no autorizadas.

- Construir centros y unidades de respuesta a incidentes: fundamentalmente los Equipos de Respuesta ante Emergencias Informáticas (CERT), que realicen una evaluación constante y proactiva de las incidencias y con responsabilidades claras, involucración de todos los actores relevantes y evaluación constante y proactiva de incidentes y competencias. Se recomienda realizar cibersimulacros en escenarios reales involucrando a todos los niveles para comprobar la capacidad de respuesta.

> *"Se recomienda realizar cibersimulacros en escenarios reales"*

- Establecer un sistema integral de comunicación que facilite el intercambio de información de amenazas o vulnerabilidades detectadas dentro de la ciudad y con otros niveles de gobierno, negocios y otros sectores.

- Potenciar la concienciación pública, educación y formación de personal mediante campañas dirigidas al público general, formación específica en ciberseguridad para empleados y mano de obra cualificada.

- Facilitar la cooperación pública, privada y académica, mediante el modelo de PPP (participación público-privada), asociación con universidades, presencia en eventos sectoriales y otras iniciativas similares.

Todo ello deberá realizarse teniendo en cuenta los retos a los que se enfrenta la ciberseguridad de forma global, entre ellos el dilema entre privacidad y seguridad, la disyuntiva entre democracia y control y el reto de garantizar la gobernanza al tiempo que se garantiza la independencia de la red y el suministro continuo.

EL MEJOR EJEMPLO DE *SMART CITY* SEGURA ES UN PAÍS

A pesar de todo lo mencionado, son pocas las ciudades que han implantado estrategias integrales que las acerque a ser consideradas smart cities auténticas según las definiciones teóricas de ciudades inteligentes. Es por ello que actualmente las soluciones y recomendaciones para lograr una ciudad inteligente cibersegura no están en disposición de ser implementadas de una forma completa. En la situación actual, resultaría más realista hablar de una implantación asimétrica del sistema inteligente, afectada a su vez por una asimetría en vulnerabilidades y amenazas.

Sin embargo, existe un caso que ilustra perfectamente la necesidad de definición de unidades básicas de ciberseguridad de pequeño tamaño. Se trata de Estonia, como recuerda *Liina Areng*: el tamaño de la población, la cercanía entre el gobierno local y el ciudadano, la proyección global gracias a Internet, la menor exposición a conflictos internacionales propios de grandes estados y la relativa facilidad para implantar soluciones innovadoras hacen del pequeño estado digital un ejemplo a seguir en ciberseguridad.

Desde 1995, Estonia informatizó todos los colegios y enseñó a los mayores del país cómo utilizar los ordenadores e Internet. En 2005 fue el primer país en tener elecciones a través de Internet. A partir de 2014, Estonia comenzó a emitir identificación digital para los no residentes. El siguiente proyecto es la creación de las "embajadas de datos", ya tratadas en el *Real Instituto Elcano y THIBER*, para lograr que las bases de datos vitales para la supervivencia del estado estén seguras.

Para garantizar la ciberseguridad y la retención de talento necesaria para ello, tras los ciberataques de 2007 Estonia creó la Liga Estoniana de Ciberdefensa, unidad voluntaria de ciberexpertos que ayudarían al gobierno a gestionar cibercrisis. La localización del Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN en Tallín en 2008 supuso otro de los hitos que confirma a Estonia como potencia en ciberseguridad. A pesar de ser un estado pequeño, en muchos aspectos lo más parecido a una *smart city* que hay actualmente en el panorama internacional, Estonia es un ejemplo a seguir en muchos casos para las grandes ciudades con vocación *smart.*

En conclusión, como afirma *Michele Acuto*, "las ciudades están a la vanguardia de los retos de seguridad actuales, especialmente cuando se trata de amenazas no tradicionales" pero, al mismo tiempo, "antes de una acción global extraordinaria, el urbanismo se trata de comprometerse con la realidad ordinaria justo en el umbral de nuestra puerta". Por ello, es fundamental una estrategia de ciberseguridad que tenga en cuenta el doble componente, local e internacional de las ciudades inteligentes, y su papel clave como unidad básica para la seguridad en el entorno cibernético.

4 Entrevista a David Barroso.
Fundador, CounterCraft.

1. David, es usted uno de los principales expertos nacionales en el ámbito de la seguridad informática. En su opinión, ¿Cuáles serán los principales retos en materia de ciberseguridad a los que deberán enfrentarse gobiernos y empresas de todo el mundo en los próximos 5 años?

Está ampliamente aceptado por todo el mundo que nos encontramos en un cambio de modelo de sociedad en todos sus aspectos, pero donde claramente la seguridad (y por extensión, la ciberseguridad) coge una relevancia especial; los sucesos principales que están ocurriendo en el mundo desde hace unos años están directamente relacionados con la seguridad (o falta de ella). Por primera vez en muchos años hay una transición hacia un entorno menos seguro, puesto que las guerras o atentados terroristas no ocurren lejos de nosotros. Todo ello tienen una componente de ciberseguridad imprescindible, y los gobiernos se encuentran en una situación muy complicada para enfrentarse a ello.

Por ejemplo recientemente hemos visto como gobiernos como el británico se están planteando la posibilidad de obligar a incluir puertas traseras el cifrado de los datos y comunicaciones, o como el gobierno francés se plantea bloquear ciertas comunicaciones en momentos de crisis.

Además, si a la dependencia casi total sobre la tecnología sumamos las malas prácticas referentes a seguridad de algunos fabricantes de hardware y software, nos encontramos en un escenario nada prometedor tanto para gobiernos como empresas. Sólo nos falta añadir a esta combinación la falta de confianza entre estados resaltada con la figura de Edward Snowden para tener un escenario complicado.

Pero todo no es tan negativo como parece; existen múltiples iniciativas tanto por parte de gobiernos como de empresas para intentar contrarrestar todas las amenazas existentes y recuperar la confianza entre todos los actores involucrados. Es claramente un desafío, pero poco a poco se verán sus resultados.

2. En diciembre de 2013 el Gobierno aprobaba la *Estrategia Nacional de Ciberseguridad* y, un año después, hacía lo mismo con el Plan Nacional de Ciberseguridad derivado de la estrategia, ¿Cuál es su opinión sobre el grado de madurez de la ciberseguridad nacional?

Todavía nos falta mucho para aterrizarlo y que sea operativo. Deberíamos adoptar las mejores prácticas y medidas positivas de otros países, e intentar dejar a un lado los intereses de cada uno.

A diferencia que las amenazas tradicionales (donde está claro el ámbito de los actores involucrados, tanto militares como policiales), en la ciberseguridad es necesario que exista una clara cooperación e involucración de entornos civiles y privados, y existe ejemplos claros. Un caso de éxito por ejemplo es el NCFTA (National Cyber-Forensics & Training Alliance) una organización sin ánimo de lucro de EEUU que aglutina la colaboración de universidades (principalmente Carnegie Mellon) con empresas privadas, para ofrecer soporte y colaboración a órganos como el FBI o el USSS (servicio secreto de EEUU).

"...en la ciberseguridad es necesario que exista una clara cooperación e involucración de entornos civiles y privados..."

A través del NCFTA se han conseguido infinidad de operaciones de éxito que acabaron con la detención de bandas de crimen organizadas.

Otro ejemplo en el que fijarse más cercano es en Holanda, donde la policía holandesa desde años cuenta en sus filas con personal civil, aparte de apoyarse en empresas privadas holandesas, que ha posibilitado la ejecución con éxito de innumerables operaciones policiales.

Por supuesto, para poder llevar a cabo el Plan Nacional de Ciberseguridad, es necesario también contar con una infraestructura adecuada que lo sustente. Hoy en día vemos a la policía judicial muchas veces totalmente desbordada y sin poder contar con los medios suficientes para poder llevar a cabo su trabajo (de hecho muchos de los éxitos de los que se presume en los medios no fueron posible sin su pasión por su trabajo y su total dedicación, y no de 8 horas diarias precisamente).

Y no sólo es presupuesto y orden, sino también dejando atrás muchos de los clichés que aún todavía perduran hoy en día.

3. España necesita una industria nacional de ciberseguridad a la vanguardia, ¿Qué medidas podrían revitalizar la industria y el sector nacional de la ciberseguridad?

La respuesta sencilla es apoyar a la industria nacional de ciberseguridad, pero creo que debemos mirar a más largo plazo. Sin llegar a compararnos a países como Israel, donde existe una maquinaria perfectamente engrasada entre gobierno, universidades y capital (inversores), debemos aprovechar el hecho de estar en Europa y llegar a compartir los esfuerzos a nivel europeo, creando una industria potente a nivel europeo.

Además es necesario acercar mucho más a las Universidades y Centros Tecnológicos a la

industria, promoviendo esas colaboraciones pero de manera más eficiente. Contamos con grandes grupos de investigación académicos pero rara vez se aprovecha su trabajo en la industria.

A nivel de empresas, una buena opción es beneficiar a nivel de impuestos a aquellas empresas que apoyan a la industria de ciberseguridad nacional (o europea), para poder incentivar a que contraten servicios o productos nacionales o europeos, ayudando a las empresas pequeñas que muchas veces no pueden competir contra las grandes corporaciones multinacionales.

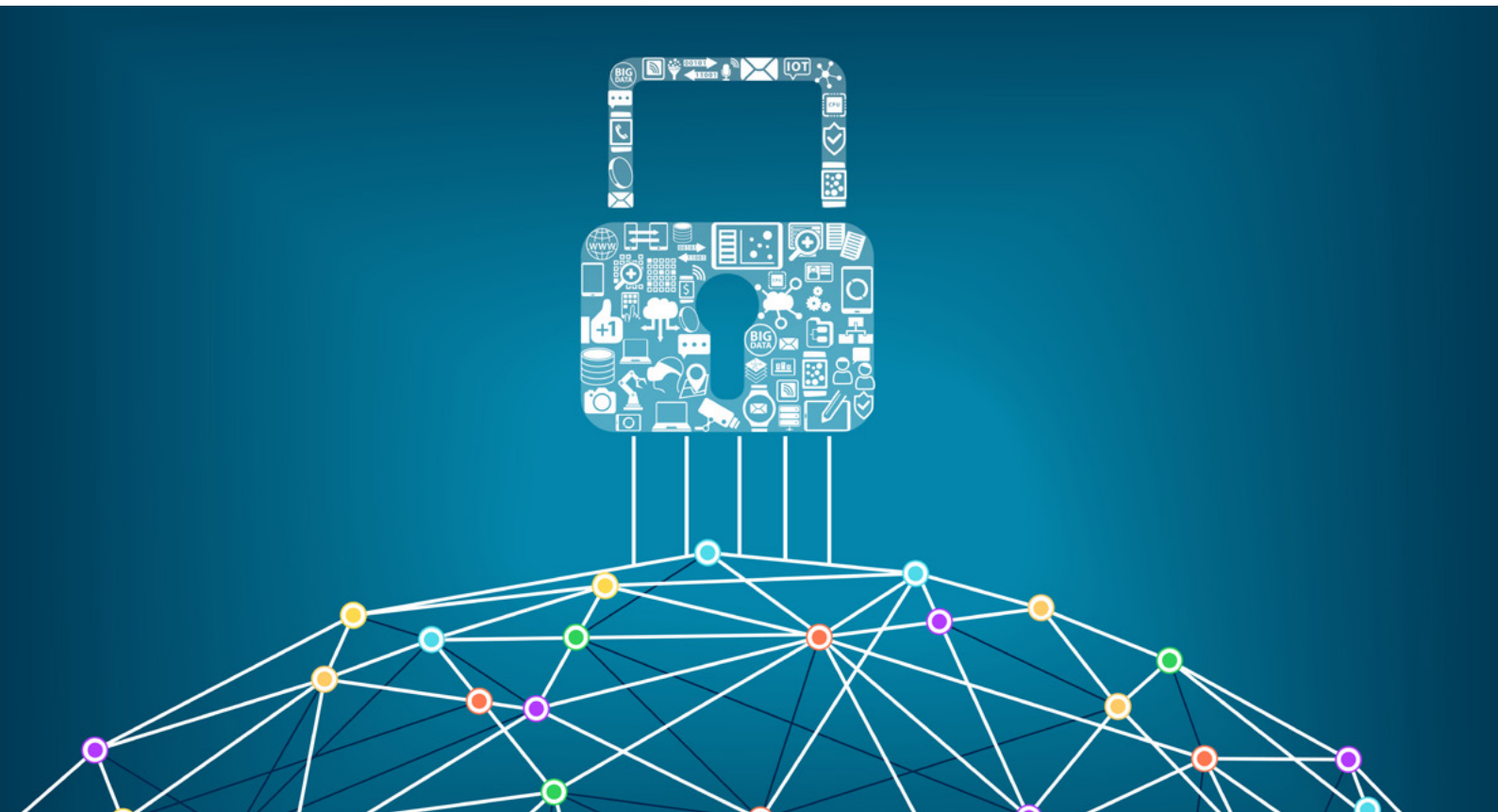
4. ¿Debería el gobierno promover una política de Coordinated Vulnerability Disclosure, también conocida como Responsible Disclosure? ¿En qué términos?

Me parece una muy buena opción si hablamos de activos pertenecientes a la Administración Pública. A nivel de gobierno existen miles de redes y dispositivos que muchas veces son vulnerables, y a la vez contamos con un talento impresionante en profesionales de seguridad.

Por supuesto este 'bug bounty' gubernamental tendría que estar perfectamente organizado y tendría que compensar económicamente a los investigadores que encontraran vulnerabilidades. Me parece una inversión mínima que podría tener unos resultados espectaculares. Muchas grandes empresas ya lo hacen y el resultado es siempre favorable (si se hace bien).

Por otro lado, también de alguna forma hay que adecuar cómo se manejan los incidentes de seguridad tanto del gobierno como de las empresas. En Europa ya hay muchas ideas al respecto sobre la notificación de incidentes de seguridad, pero no estaría mal que España tomara la responsabilidad del tema en Europa.

Es un caso parecido con el Arreglo de Wassenaar y su relación con las herramientas de ciberseguridad. Aprovechando que España aún preside el Arreglo, es una oportunidad perfecta para tomar el liderazgo en estos temas.



5. ¿Considera que existen los mecanismos necesarios para una colaboración internacional efectiva en la lucha contra el cibercrimen? ¿Cómo podría mejorarse?

Claramente no. Muchos incidentes y delitos son muy complejos no sólo técnicamente, sino que afectan a la jurisdicción de varias naciones, con lo que nos chocamos con procesos burocráticos interminables que limitan claramente las investigaciones.

Aunque existan intentos para mejorar la colaboración, muchos de ellos se quedan en papel, puesto que no es nada sencillo; es verdad que hay avances sobre ello, y el rol más operativo que está adquiriendo por ejemplo Europol es uno de ellos, pero si hay que dialogar o cooperar con otros países muchas veces los procesos son lentos y burocráticos, cuando los incidentes de ciberseguridad necesitan una inmediatez absoluta.

Por suerte, muchas veces se buscan atajos para evadir esa burocracia que permite que exista una colaboración internacional más eficiente.

6. Para terminar, ¿Cuáles serian las líneas maestras de un Plan Nacional de Ciberseguridad elaborado por Ud.?

Buscaría el consenso y la colaboración con países europeos para hacer un esfuerzo común, distribuyendo los ejes principales entre todos ellos, siendo los principales:

- Apoyo a la creación de tecnología de ciberseguridad (I+D+i, inversiones, etc.)
- Sincronización del mundo académico con la industria.
- Ajuste de los marcos jurídicos y reglamentarios.
- Involucración de las presidencias de los gobiernos.
- Formación de profesionales cualificados.
- Simbiosis del mundo militar, FCSE con empresas privadas y civiles.
- Protección de infraestructuras críticas.
- Definir roles y responsabilidades de CERTs, así como promover su colaboración.

Como he comentado anteriormente, no intentaría reinventar la rueda, sino en la primera fase simplemente fijarnos en los aspectos positivos de otras naciones para poder realizar lo mismo; si conseguimos esta primera fase, ya tendremos muchos hitos alcanzados.

5 Informes y análisis sobre ciberseguridad publicados en noviembre de 2015

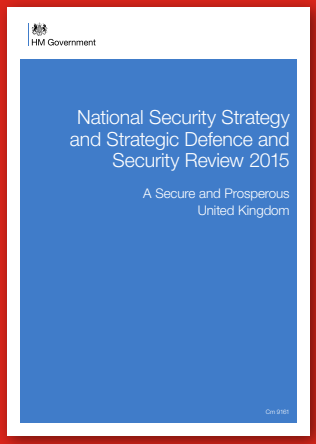
Medidas de Seguridad en Telefonía Móvil (CCN-CERT)

Security and Resilience of Smart Home Environments (ENISA)

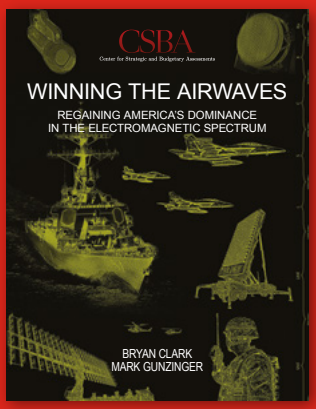
Despega la transformacion digital del Ministerio de Defensa (IEEE)

U.S – Japan Cooperation in Cybersecurity (CSIS)

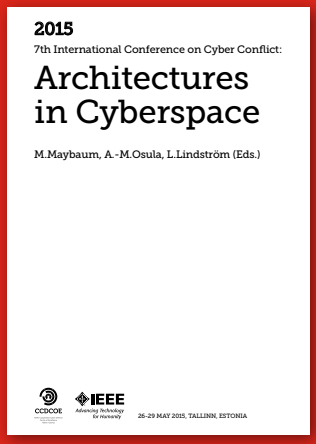
National Security Strategy and Strategic Defence and Security Review 2015 (UK



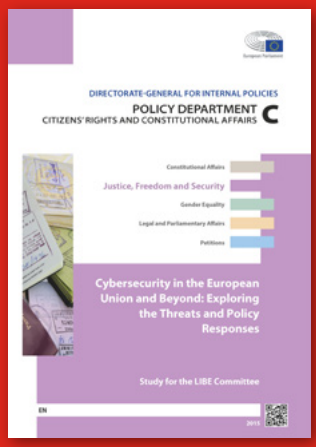
Wining the Airwaves (CSBA)



Architectures in Cyberspace (CCDCOE)



Cybersecurity in the European Union (European Union)



6 HERRAMIENTAS DEL ANALISTA: IntelMQ

IntelMQ es una solución diseñada para los Centro de Respuesta ante Incidentes (CERTs) así como para unidades de ciberinteligencia o inteligencia de amenazas, usado para la recolección y el procesamiento de feeds de seguridad, pastebins, tweets, etc. Mediante el uso de colas de mensajes. Es una iniciativa impulsada por el *IHAP (Incident Handling Automation Project)* que fue diseñado conceptualmente por los CERT europeos durante varios eventos de seguridad.

Su meta principal es la de dotar a los equipos de respuesta a incidentes, de los medios adecuados para recolectar y procesar información sobre inteligencia de amenazas, mejorando el proceso de gestión de ciberincidentes.

IntelMQ tiene una estructura modular basada en robots. Hay cuatro tipos de robots:

- CollectorBots, que recuperan datos de fuentes internas o externas, dando como resultado los informes que constan de muchos conjuntos de datos individuales.
- ParserBots, que analizan los datos dividiéndolos en eventos individuales con una estructura definida y normalizada, usando una ontología de armonización.
- ExpertBots, que enriquecen los eventos existentes, por ejemplo, revertiendo registros, buscando información de ubicación geográfica o los contactos de abuse.
- OutputBots, que escriben eventos en los archivos, bases de datos, APIs, etc.

Cada robot tiene una cola de origen (excepto los collectors) y puede tener múltiples colas de destino (con excepción de los Output). Pero múltiples robots pueden escribir en la misma cola, lo que resulta en múltiples entradas para otro bot. Cada bot se ejecuta en un proceso independiente siendo identificables por un identificador de bot.

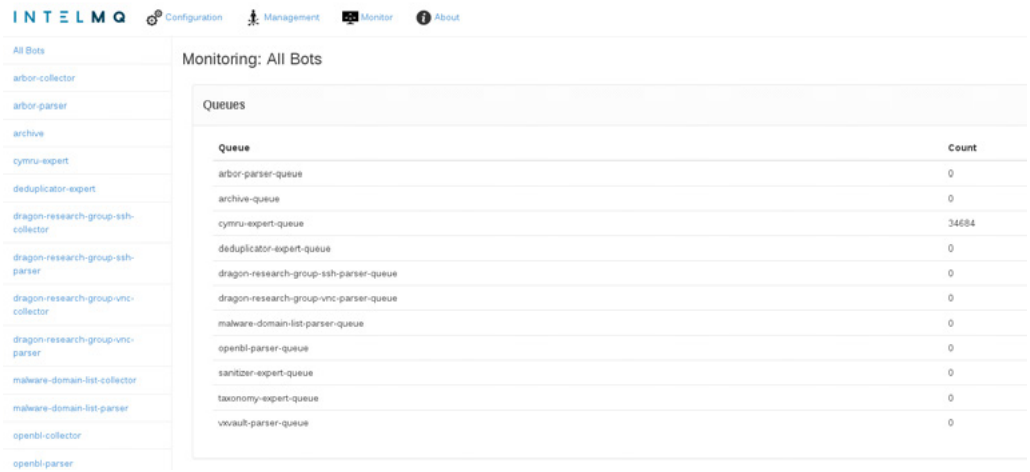


Ilustración 1 Listado mensajes provenientes de un listado de bots en IntelMQ

Adicionalmente, IntelMQ tiene una herramienta llamada IntelMQ Manager que otorga al usuario una manera fácil de configurar todos los flujos de trabajo y los bots. Se recomienda usar el Administrador IntelMQ para familiarizarse con las funcionalidades y los conceptos de la herramienta. IntelMQ Manager tiene todas las posibilidades de la herramienta intelmqctl y tiene una interfaz gráfica para la puesta en marcha y configuración de la herramienta.

Aunque el diseño de IntelMQ fue influenciado por AbuseHelper, ha sido re-escrito desde cero teniendo por objeto:

- Reducir la complejidad de la administración del sistema anterior.
- Reducir la complejidad de escribir nuevos robots para nuevas fuentes de datos.
- Reducir la probabilidad perder información o eventos en todo el proceso con la funcionalidad de persistencia (incluso caída del sistema).
- Usar y mejorar la Ontología de armonización de datos existente.
- Representar todos los mensajes en formato JSON.
- Integrar herramientas existentes y descritas en otros número de CIBERelcano, como CIF o AbuseHelper.
- Proporcionar una manera fácil de almacenar datos en recolectores de logs tales como Elasticsearch, Splunk, etc.
- Proporcionar una manera fácil de crear listas negras propias.
- Proporcionar una comunicación sencilla con otros sistemas a través de una API HTTP RESTful.

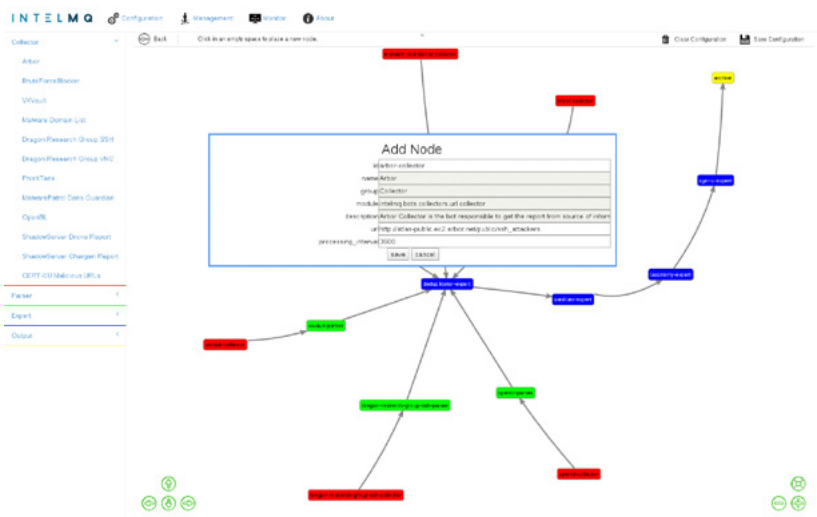


Ilustración 2 Ejemplo de configuración de un bot

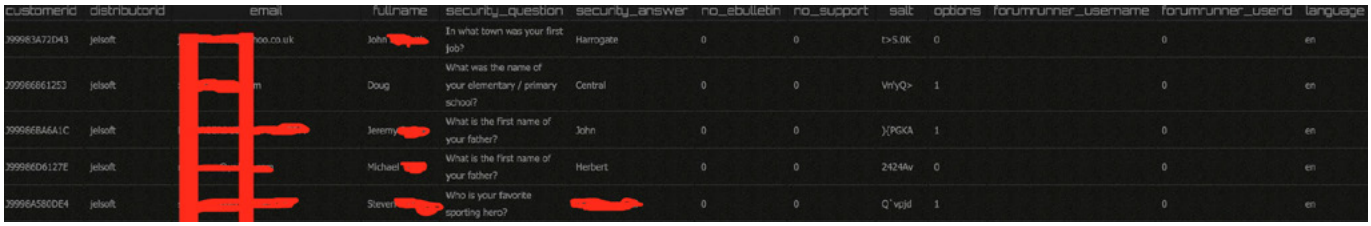
7 Análisis de los Ciberataques del mes de noviembre de 2015

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

CIBERCRIMEN

A comienzos de mes, un asaltante autodenominado *Coldzer0 afirmó* haber vulnerado Vbulletin.com obteniendo los detalles de 479.895 usuarios empleando una vulnerabilidad de día cero.

El mismo usuario Coldzer0 también *afirmó haber hackeado el foro de FoxIt* utilizando el mismo 0-day con idénticos resultados.



customerid	distributordid	email	fullname	security_question	security_answer	no_vbulletin	no_support	salt	options	forumrunner_username	forumrunner_userid	language
999983A72D43	jelsoft	[redacted]	John [redacted]	In what town was your first job?	Harrogate	0	0	t>5.0K	0		0	en
999966861253	jelsoft	[redacted]	Doug	What was the name of your elementary / primary school?	Central	0	0	VrlyQ>	1		0	en
999986BA6A1C	jelsoft	[redacted]	Jeremy [redacted]	What is the first name of your father?	John	0	0	)(PGKA	1		0	en
999986D6127E	jelsoft	[redacted]	Michael [redacted]	What is the first name of your father?	Herbert	0	0	24244v	0		0	en
99996A580DE4	jelsoft	[redacted]	Steven [redacted]	Who is your favorite sporting hero?	[redacted]	0	0	Q`vcjd	1		0	en

Ilustración 1 Muestra del dump de contraseñas de Vbulletin.com

```
From: "Armada Collective" armadacollective@openmailbox.org
To: abuse@victimdomain; support@victimdomain; info@victimdomain
Subject: Ransom request: DDOS ATTACK!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins @ XXX

When we say all, we mean all - users will not be able to access sites host with you at
all.

Right now we will start 15 minutes attack on your site's IP (victims IP address). It
will not be hard, we will not crash it at the moment to try to minimize eventual damage,
which we want to avoid at this moment. It's just to prove that this is not a hoax. Check
your logs!

If you don't pay by Friday , attack will start, price to stop will increase to 40 BTC
and will go up 20 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name,
instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap
protection will help.

Prevent it all with just 20 BTC @ XXX

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL
NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.
```

Ilustración 2 Carta de rescate enviada por Armada Collective

Durante los primeros veinte días del mes, tuvo lugar una gran oleada de ataques DDoS, especialmente focalizados en servicios de correo electrónico, como *FastMail*, *NeoMailbox*, *RunBox*, *ProtonMail*, *HushMail* o *Zoho*. En cuatro de los casos anteriores, la autoría era reclamada por un grupo denoninado Armada Collective. Dicho grupo solicitaba a los titulares de los servicios el pago de un rescate en bitcoins a fin de finalizar el ataque o, en caso contrario aumentaría el alcance del DDoS. ProtonMail pagó el rescate de 15 Bitcoins (unos 6.000 $), sin embargo no cesó de recibir el citado altísimo tráfico de red.

En cuanto a las direcciones Bitcoin especificadas por los atacantes en los correos electrónicos a ProtonMail y Runbox, son las mismas, lo que demuestra que los ataques están efectivamente vinculados.

El 8 de *noviembre los servidores del ejército brasileño fueron infiltrados* por unos asaltantes desconocidos conllevando la exposición de datos personales (números de la Seguridad Social y contraseñas principalmente) de unos 7.000 agentes. El ataque parece haber sido incitado como represalia contra la conducta supuestamente inadecuada de un equipo del ejército durante un concurso de Captura la Bandera (CTF) en un evento de ciberseguridad en el Centro del Gobierno de Defensa Cibernética de Brasil.

Este mes también se hacía pública la noticia de que un hacker denominado Orion trató de vender 200.000 credenciales válidos de Comcast que él afirma que robó en 2013 del servidor de correo, entonces vulnerable, de la empresa de telecomunicaciones.

La compañía de telecomunicaciones restableció las contraseñas de las cuentas afectadas tras de la noticia. Las credenciales estaban siendo vendidas en un market en la deep web denominado Python Market.

Del conjunto total de 590.000 cuentas a la venta por 1.000 $, según la compañía, solo alrededor de un tercio eran válidas.

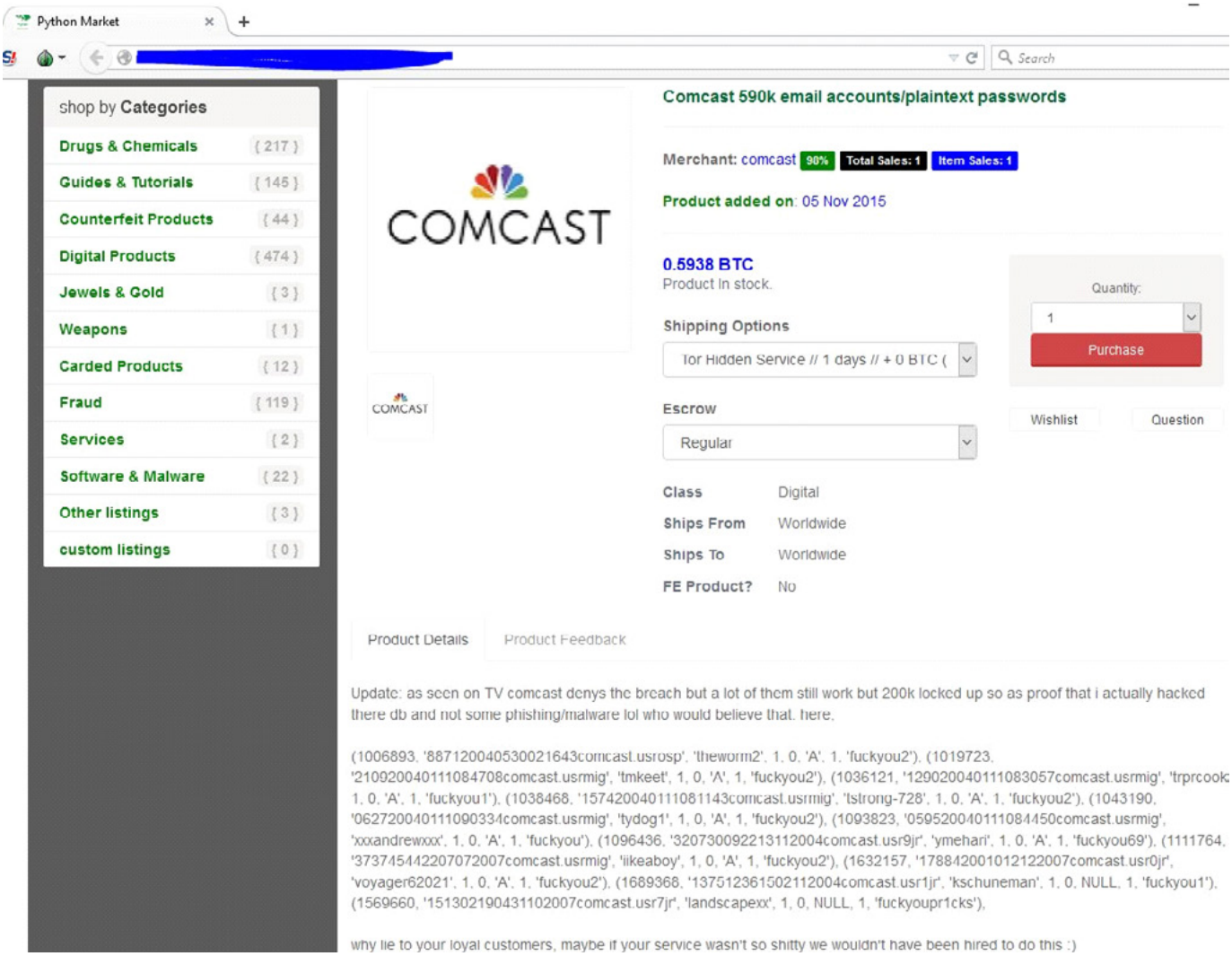


Ilustración 3 Credenciales de Comcast a la venta en la deep web

CIBERESPIONAJE

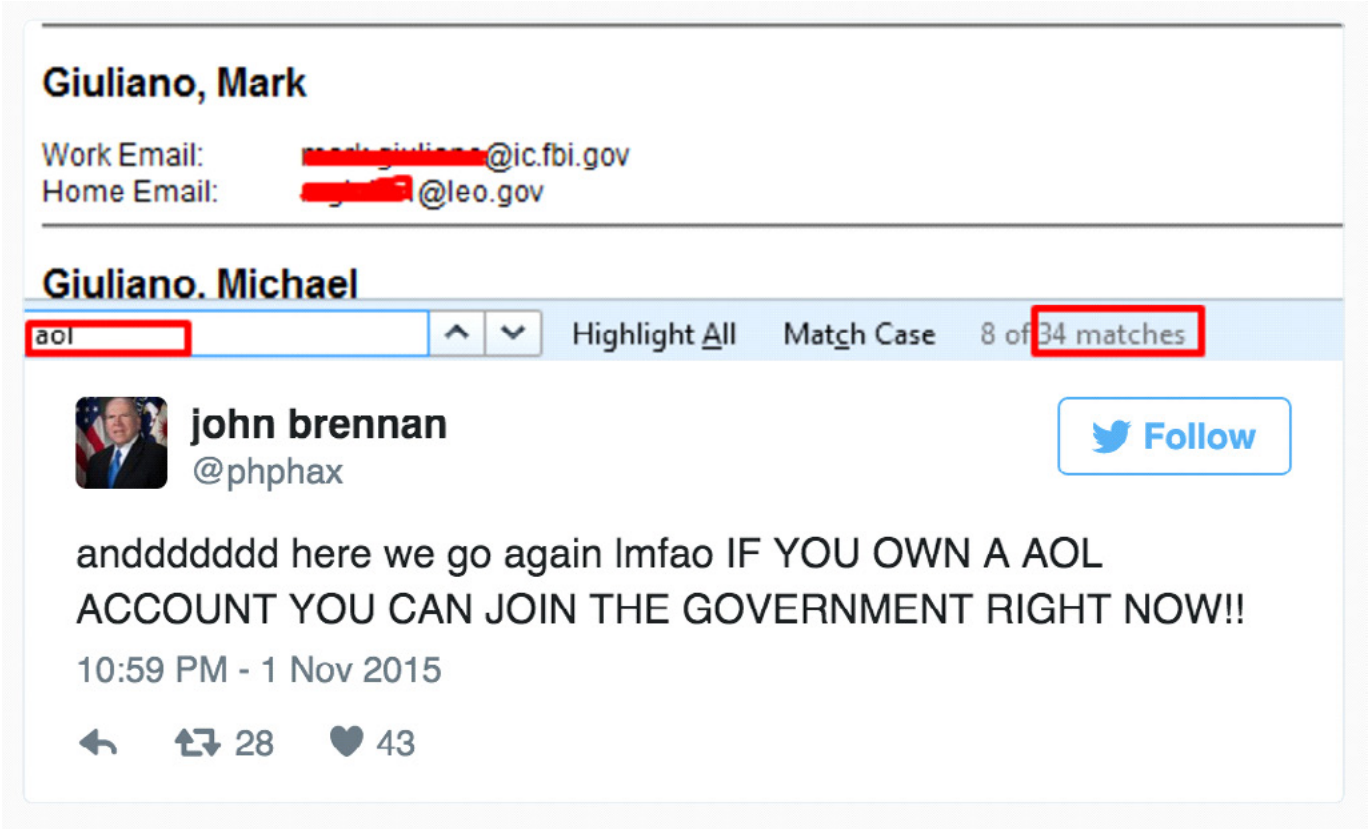
En el plano del ciberespionaje, *el Wall Street Journal reveló* que diversas cuentas de correo electrónico y de redes sociales de altos funcionarios del gobierno de Obama fueron hackeados recientemente por miembros de la Guardia Revolucionaria de Irán.

Los ataques se cree que están conectados a la reciente detención en Teherán del empresario iraní-estadounidense Siamak Namazi, que había presionado para que las relaciones económicas y diplomáticas fuesen más sólidas y fluidas entre los EE.UU. e Irán.

HACKTIVISMO

La primera semana de noviembre, el grupo de hackers adolescentes que en teoría se infiltraron en la cuenta de correo electrónico del director de la CIA, John Brennan, han comunicado que actualmente están focalizando sus esfuerzos en otros funcionarios del gobierno norteamericano, en este caso alegan haber vulnerado una cuenta de correo electrónico del subdirector del FBI, Mark Giuliano.

El grupo, que se autodenomina "Crackas with Attitude" ya está siendo investigado por el FBI, tras haber publicado su último logro en Twitter. Uno de los miembros, llamado Cracka, envió capturas de pantalla que demostraban tener control sobre el buzón de correo y, además, afirmó haber llamado un número de móvil perteneciente a Giuliano.



Durante este mes, Anonymous ha continuado con la *operación de descubrimiento de miembros del ku kux klan, denominada #opKKK* comenzada hace un par de meses. En esta ocasión, el grupo hacktivista publicó en PasteBin, enlaces a grupos en redes sociales del KKK, nombres, perfiles de Facebook y G+, ubicaciones, datos personales, incluyendo conexiones familiares de los miembros del KKK, alias y cargo en el grupo. Las identidades de varios Imperial Wizards (suerte de líderes del KKK, también se han hecho públicos.

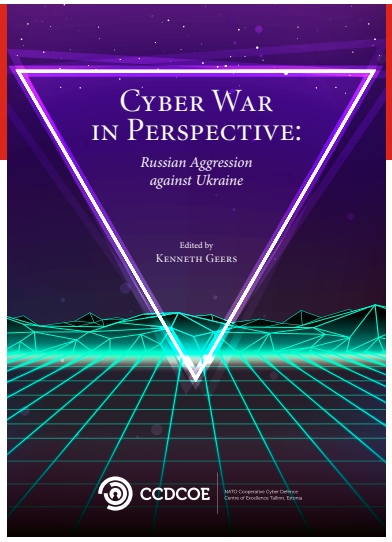
Sin embargo, tras los atentados cometidos en la noche del 13 de noviembre en la capital francesa y su suburbio de Saint-Denis, perpetrados en su mayoría por atacantes suicidas asociados al Daesh en los que murieron 137 personas y otras 415 resultaron heridas, Anonymous y lanzó la campaña #OpParis para combatir la presencia del grupo terrorista en redes sociales e internet en general. Dos días después de los atentados, Anonymous declaró haber identificado y eliminado más de 5.500 cuentas de Twitter del grupo terrorista, publicando un manual para aquellas personas que *quisiesen unirse a su causa en la lucha contra el Daesh para eliminar su rastro de internet.*

8 Recomendaciones

8.1 Libros y películas

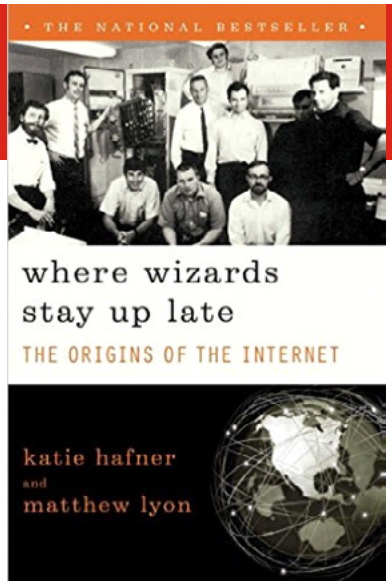
Película:
STAR WARS: EPISODIO VII - EL DESPERTAR DE LA FUERZA

Sinopsis: Esta nueva entrega de la Guerra de las Galaxias se establecerá 30 años después de 'El retorno del Jedi', contando con una nueva generación tanto de héroes como de oscuros villanos y, por supuesto, la vuelta de algunos de los personajes favoritos de los fans.



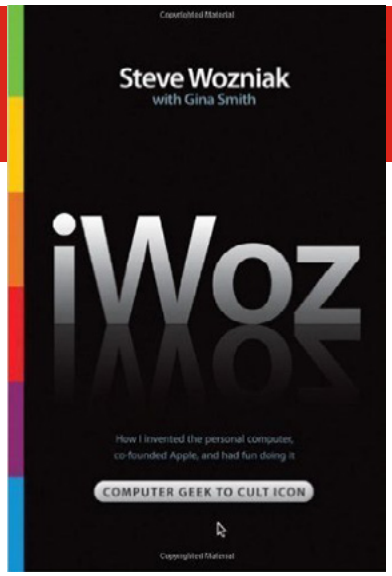
Libro:
CYBERWAR IN PERSPECTIVE

Autor: Kenneth Geers
Num. Paginas: 175
Editorial: NATO CCDCOE Publications
Año: 2015
Precio: Gratuito
Sinopsis: El CCDCOE recaba la opinion de multiples expertos internacionales para realizar un pormenorizado análisis sobre las consecuencias en el ámbito cibernético de la invasión rusa de Ucrania.



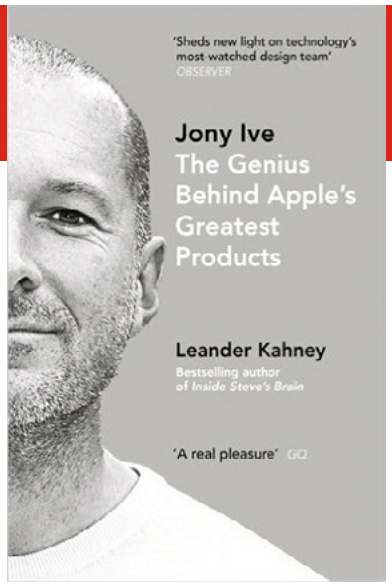
Libro:
WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET

Autor: Katie Hafner & Matthew Lyon
Num. Paginas: 304
Editorial: Simon & Schuster
Año: 1998
Precio: 11.50 Euros
Sinopsis: Los autores, a través de testimonios de sus principales protagonistas, nos cuentan la gran aventura del nacimiento de Internet.



Libro:
IWOZ BY STEVE WOZNIAK

Autor: Steve Wozniak
Num. Paginas: 352
Editorial: Headline Review
Año: 2007
Precio: 10.00 Euros
Sinopsis: Steve Wozniak narra en primera persona como lidero desde Apple -la compañía que fundo junto a Steve Jobs- la revolución informática durante la década de 1970.



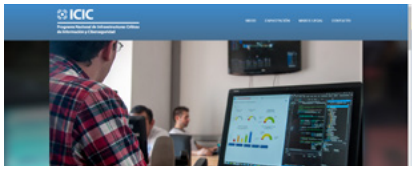
Libro:
JONY IVE: THE GENIUS BEHIND APPLE'S GREATEST PRODUCTS

Autor: Leander Kahney
Num. Paginas: 320
Editorial: Portfolio Penguin
Año: 2014
Precio: 16.00 Euros
Sinopsis: Este libro narra la historia de uno de las personas mas importantes de la historia de Apple, Jony Ive, el diseñador de los productos mas emblemáticos del gigante tecnológico.

8.2 Webs recomendadas

http://ent.siteintelgroup.com/Dark-Web-Cyber-Security/
Area de Ciberseguridad del grupo de inteligencia SITE

http://www.icic.gob.ar/index.html
Sitio web del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad de Argentina



http://www.colcert.gov.co/
Sitio web del Centro de Respuesta a Emergencias Cibernéticas de Colombia.

http://www.dsn.gob.es/sistema-seguridad-nacional/comit%C3%A9s-especializados/consejo-nacional-ciberseguridad
Sitio web del Consejo Nacional de Ciberseguridad.

http://www.ccp.gov.co/
Sitio web del Centro Cibernetico Policial de Colombia

http://www.state.gov/s/cyberissues/
Área de ciberseguridad del Departamento de Estados de los Estados Unidos.

8.3 Cuentas de Twitter

@gwcchs

@SITE_CYBER

@State_Cyber

@CyberSecInt

@CyberSkillsUK

9 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
1 diciembre	Londres	IoT Security Foundation	IoT Security Foundation Conference	https://iotsecurityfoundation.org/event/iot-security-foundation-conference/
2-17 diciembre	Garmisch-Partenkirchen, Alemania	Marshall Center	Program on Cyber Security Studies (PCSS)	http://www.marshallcenter.org/mcpublicweb/nav-main-wwd-res-courses-pcss-en.html
2 diciembre	Londres	Whitehall Media	Enterprise Security and Risk Management	http://www.whitehallmedia.co.uk/esrm/
7-8 diciembre	Londres	TechCrunch Disrupt	Disrupt London 2015	http://techcrunch.com/event-info/disrupt-london-2015/
8-10 diciembre	Omni Montelucia Resort, Scottsdale, AZ, Estados Unidos	Black Hat	Black Hat I Executive Summit	https://www.blackhat.com/exec-15/
9-11 diciembre	Arlington, Virginia, Estados Unidos	Military Networks	Cyber Security for Government	http://www.cybersecuritygovernment.com/
10-11 diciembre	Madrid	CCN	IX Jornadas STIC- CERT	http://www.redseguridad.com/eventos/agenda-del-sector/ix-jornadas-stic-cert
11 diciembre	Madrid	Seguritecnia	XXIX Trofeos Internacionales de la Seguridad	http://www.redseguridad.com/eventos/agenda-del-sector/xxix-trofeos-internacionales-de-la-seguridad
14 diciembre	Londres	IEEE	The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015)	http://www.icitst.org/
14 diciembre	Londres	IEEE	The World Congress on Industrial Control Systems Security (WCICSS-2015)	http://www.wcicss.org/
16 diciembre	Madrid	CCI	Encuentro de la Voz de la Industria	https://www.cci-es.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