ENERO 2016 / Nº 10

CIBER elcano

REAL INSTITUTO elcano ROYAL INSTITUTE

Desarrollado por:

THIBER

INFORME MENSUAL DE CIBERSEGURIDAD

REAL INSTITUTO
elcano
ROYAL INSTITUTE

Copyright y derechos:

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank

Índice

1 COMENTARIO CIBERELCANO
La ciber-soberanía china

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

Fuente: China Daily

EL pasado diciembre, la ciudad china de Wuzhen acogió la *Conferencia Mundial de Internet* (WIC). La WIC, un evento organizado por la Administración del Ciberespacio de China (CAC) desde 2014, congregó a cerca de dos mil representantes procedentes de un centenar de países. Entre los asistentes se hallaban ilustres invitados como el Primer Ministro ruso Andrei Medveded, el Presidente de Pakistán Mamnoon Hussain o los vicepresidentes de Apple, IBM o Microsoft. Paradójicamente, no participó ningún representante oficial de la alianza Five Eyes, compuesta por Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda.

La conferencia inaugural de la WIC corrió a cargo del Presidente chino Xi Jinping. En ella subrayó la importancia estratégica que tiene la seguridad del ciberespacio para el desarrollo socio-económico chino. Además, compartió con los asistentes la visión que tiene su gobierno sobre el futuro del ciberespacio, centrando su discurso en tres áreas fundamentales: gobernanza del ciberespacio, ciberseguridad y ciber-soberania.

En relación a la primera, el presidente abogó por un ciberespacio regulado. No obstante, advirtió que sus reglas de gobernanza deberían ser consensuadas por la comunidad internacional y no impuestas por un solo actor, en clara alusión a Washington. Esta misma idea fue defendida por Lu Wei, ciberzar chino y director del CAC, durante el discurso de clausura del WIC.

En materia de ciberseguridad, el presidente chino expuso la necesidad de evitar la militarización del ciberespacio e instó a la comunidad internacional a mantener un "comportamiento civilizado" en este dominio. Asimismo, realizó un llamamiento a la comunidad internacional para implementar los mecanismos necesarios para luchar de manera efectiva contra el cibercrimen. En este sentido, puso como ejemplo los recientes acuerdos alcanzados en materia de ciberseguridad con Estados Unidos.

Finalmente, en materia de ciber-soberania, Xi subrayó que *"el principio de la igualdad soberana consagrado en la Carta de las Naciones Unidas es una de las normas básicas en las Relaciones Internacionales contemporáneas. Cubre todos los aspectos de las relaciones entre estados, incluyendo también el ciberespacio"*. Además, concluyó su discurso sentenciando que "se debe respetar el derecho de cada país a elegir de forma independiente el modo en el que quiere desarrollar su ciberespacio específico, su modelo de regulación cibernética y garantizar una participación igualitaria en la gobernanza ciberespacio internacional".

"el presidente chino expuso la necesidad de evitar la militarización del ciberespacio"

Con el objetivo de garantizar la continuidad de WIC, el gobierno chino ha constituido un comité asesor de alto nivel copresidido por Fadi Chehade, director ejecutivo de la *Corporación de Internet para la Asignación de Nombres y Números* (ICANN) y Jack Ma, fundador del gigante chino de Internet *Alibaba*, al que en las próximas fechas se unirán una treintena de reconocidos expertos mundiales en el ámbito de Internet.

En definitiva, no cabe duda de que el ciberespacio se ha convertido, desde hace varios años, en una prioridad estratégica para las principales potencias mundiales. Sin embargo, todavía quedan gobiernos que obvian el valor que posee esta dimensión para ejercer poder y condenan a sus naciones tanto a la insignificancia cibernética como a la irrelevancia política y socioeconómica.

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
El Reglamento y la Directiva de Protección de Datos: Nuevas reglas del juego para la seguridad de la información personal europea

AUTORA: Paula Hernández. Analista de THIBER y Senior Associate of Governance, Risk & Compliance de Ecix Group.

Ya podemos poner fecha aproximada a la entrada en vigor de las nuevas normativas europeas en materia de protección de datos. Y es que, tras años de negociaciones y varias propuestas, a finales de 2015, el Parlamento Europeo y el Consejo alcanzaron un acuerdo sobre la reforma propuesta por la Comisión. Previéndose una publicación en el Diario Oficial para el primer trimestre de 2016, entrando en vigor a los 20 días de su publicación, y dado inicio a un periodo de dos años para su aplicación. Es decir, **exigible a partir de 2018.**

El paquete normativo consta de dos propuestas legislativas:

- una propuesta de Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (**Reglamento General de Protección de Datos**, o GDPR, por sus siglas en inglés), y
- una propuesta de Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y a la libre circulación de estos datos **(Directiva sobre protección de datos tratados por las autoridades policiales y judiciales).**

"el Parlamento Europeo y el Consejo alcanzaron un acuerdo sobre el Reglamento de protección de datos"

Si bien aún hay infinidad de cuestiones por definir, a continuación exponemos algunas pinceladas de aspectos relevantes de ambas regulaciones.

Reglamento general de protección de datos:

Respecto del **Reglamento**, su impacto viene ya desde su conformación como norma jurídica de alcance general y aplicación directa, es decir, desde su entrada en vigor será exigible en todos los estados miembros de la Unión. **El tratamiento de datos personales en toda la Unión Europea se regirá por la misma normativa.**

Recordemos que a día de hoy el tratamiento de nuestros datos se regula por unos principios derivados de la **Directiva**, transpuestos a nuestro ordenamiento jurídico a través de una norma nacional la LOPD, que define cómo garantizar dichos principios.

El Reglamento General de Protección de Datos o GDPR, dibuja un escenario más actualizado, coherente y dotado de una mayor seguridad jurídica para los agentes implicados, lo que redunda tanto en la confianza de los ciudadanos respecto de la protección de su intimidad como en un mercado más competitivo, donde un sistema de *ventanilla única* o *one-stop-shop* hará las veces de catalizador del proceso de reforma.

Los requisitos exigidos por la normativa serán de aplicación no solo a aquellas empresas con sede en el territorio europeo, sino a cualquiera que ofrezca bienes o servicios a ciudadanos europeos, incluso gratuitos, (p.e. a través de *website*), o lleve a cabo acciones de monitorización de usuarios europeos (p.e. mediante *cookies* o mecanismos análogos).

Son muchas las novedades que incluye la propuesta. **Medidas jurídicas** -como el Derecho al olvido, el Derecho a la portabilidad, matices al consentimiento, mayores garantías para las transferencias internacionales-, **medidas organizativas** -como la designación de un *Data Privacy Officer* o Delegado de protección de datos cuando así se requiera, la implantación de conceptos como el *Privacy by design and by default* o programas de certificación- o **medidas técnicas** – como la adopción de medidas de seguridad adecuadas a riesgo o gestión de brechas- que sin duda tendrán un gran impacto en los procesos de las organizaciones.

A los efectos de este artículo vamos a exponer algunas pinceladas de **exigencias técnico-organizativas relevantes que en materia de seguridad de la información personal** introduce el GDPR:

Seguridad de los datos: será necesario adecuar las medidas a los riesgos a los que se encuentre expuesta la información, garantizando con carácter general la confidencialidad, integridad y disponibilidad y concretamente la destrucción accidental o ilícita, la comunicación no autorizada o el acceso ilícito a datos transmitidos o almacenados.

Comunicación de brechas de seguridad: se establece la obligación de notificar a la autoridad de control en un plazo máximo de **72 horas**, desde que tenga constancia, cualquier violación de datos de carácter personal.

La comunicación deberá incluir información acerca de:

- La naturaleza de la violación (categorías, número de afectados, y categorías y número de registros de datos);
- La identidad y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
- Las consecuencias derivadas del incidente
- Las medidas propuestas o adoptadas para remediarlo.

Asimismo, especial relevancia reviste la exigencia de una eventual comunicación de la violación de datos o brecha de seguridad al interesado, cuando ésta conlleve un alto riesgo para los derechos y libertades individuales. No será necesario llevar a cabo dicha comunicación siempre que el responsable demuestre, a satisfacción de la autoridad de control, que ha implementado medidas de protección tecnológica apropiadas y que se han aplicado a los datos afectados. En aquellos casos en que la comunicación directa al interesado conlleve un esfuerzo desproporcionado, se deberá llevar a cabo una comunicación pública que permita a los afectados recibir la información.

Registro de tratamiento de datos: se hace necesario elaborar un registro de tratamiento de datos con identificación de: (i) responsable del fichero y del *Data Privacy Officer*, (ii) Finalidad, (iii) Categorías de datos, (iv) Categorías de destinatarios, (v) Transferencias internacionales, (vi) plazos de conservación y (vii) Medidas de seguridad.

Evaluación de impacto de la privacidad: -o PIA, por sus siglas en inglés-, que requiere de un análisis de impacto antes de llevar a cabo determinados tratamientos de alto riesgo, de los resultados del análisis se derivarán las medidas a adoptar para el tratamiento en cuestión.

Se definirán supuestos en que deberá llevarse a cabo de forma preceptiva dicho análisis (p.e. tratamientos sistemáticos con finalidades de análisis de perfiles o comportamiento, decisiones automatizadas, tratamientos a gran escala sobre datos sensibles o videovigilancia a gran escala) y también podrán establecerse aquellos supuestos en los que no deberá llevarse a cabo.

Los requisitos mínimos que debería incluir la evaluación serían, en particular:

- Descripción general de las operaciones de tratamiento previstas, finalidades, y, en su caso, el interés legítimo perseguido;
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento en relación con la finalidad;
- Una evaluación de los riesgos para los derechos y libertades de los interesados;
- Las medidas previstas para hacer frente a los riesgos, así como las garantías y medidas de seguridad destinadas a garantizar la protección de datos personales y a evidenciar el cumplimiento.

El régimen sancionador recogido por el Reglamento prevé **multas de hasta 20 millones de euros o el 4% de la facturación mundial anual del ejercicio anterior,** (la cifra que resulte más alta).

Directiva sobre protección de datos tratados por las autoridades policiales y judiciales:

Las necesidades cada vez mayores en materia de prevención y lucha contra el terrorismo y la delincuencia transnacionales, hacen necesaria la cooperación, y con ello un rápido movimiento de información personal, entre las distintas autoridades policiales y judiciales europeas.

En este caso se busca la armonización a través de una Directiva, dejando flexibilidad a los estados para aplicar los principios, normas y exenciones, para proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, garantizando un alto nivel de seguridad pública, y asegurar el intercambio de datos personales entre las autoridades competentes dentro de la Unión.

Como novedades destacables la propuesta se aplica tanto al tratamiento transfronterizo como nacional, se establecen normas sólidas para las transferencias internacionales, y se prevé un grupo consultivo conformado por el Consejo Europeo de Protección de Datos, (establecido por el GDPR), representantes de las autoridades policiales y judiciales de los Estados miembros, así como por representantes de Europol y Eurojust.

Respecto de régimen sancionador serán los estados miembros quienes en su transposición determinen las infracciones y sanciones oportunas. Dicha transposición deberá llevarse a cabo en un periodo no superior a dos años desde su publicación en el Diario Oficial de la Unión Europea, aproximadamente en 2018.

"la propuesta se aplica tanto al tratamiento transfronterizo como nacional,"

3 OPINIÓN CIBERELCANO

Explotación del ciberespacio por parte de la Rusia de Putin como elemento para ejercer poder.

AUTOR: Enrique Martín. Analista de THIBER

Desde el fin de la guerra fría la polarización del poder se había trasladado a los países occidentales liderados por Estados Unidos. La sensación de incertidumbre que los rusos tenían desde la caída de la Unión Soviética, la baja popularidad de Boris Yeltsin y varios años de caída en la influencia internacional por parte de Rusia, hicieron que Vladímir Putin con su llegada al poder en 1999, fuera visto como el líder capaz de volver a poner a Rusia y a los rusos en el primer plano del orden internacional.

Lo que el pueblo no quiso ver fue el control de los medios de comunicación como medida de manipulación principalmente interna.

Un esfuerzo para fortalecer la posición económico-militar de una nación puede favorecerse por el debilitamiento de la situación económica del adversario.

La guerra económica se puede usar para conseguir uno de los siguientes objetivos:

- Reducir el poder militar y político de un adversario, para quitarlo del tablero en un posible conflicto en curso o futuro.
- Influir en cambios de política del adversario por las dificultades que le puedan producir los efectos de la guerra económica.
- Incluso producir el suficiente descontento popular como para poner contra las cuerdas al régimen adversario.

"La ciber capacidad rusa no reside exclusivamente en las unidades militares, sino también en el crimen organizado o hackers individuales"

Con el ciberespacio, las guerras económicas son más fáciles y menos costosas teniendo un impacto mucho mayor con menos medios. Entre las principales diferencias con la guerra tradicional encontramos:

- Los ataques pueden llevarse a cabo sin tener que operar en el territorio de la víctima.
- La víctima puede tener más dificultades para atribuir el ataque, lo que inhibe cualquier represalia.
- Los efectos de un ataque puede ser mucho mayor (propiedad intelectual, infraestructuras críticas…).

Una vez que los estados han basado su entramado financiero, industrial y de infraestructuras en capacidades cibernéticas, se hacen vulnerables a los ataques ciber. De

ahí la necesidad de políticas de Ciberseguridad nacionales para protegerse.

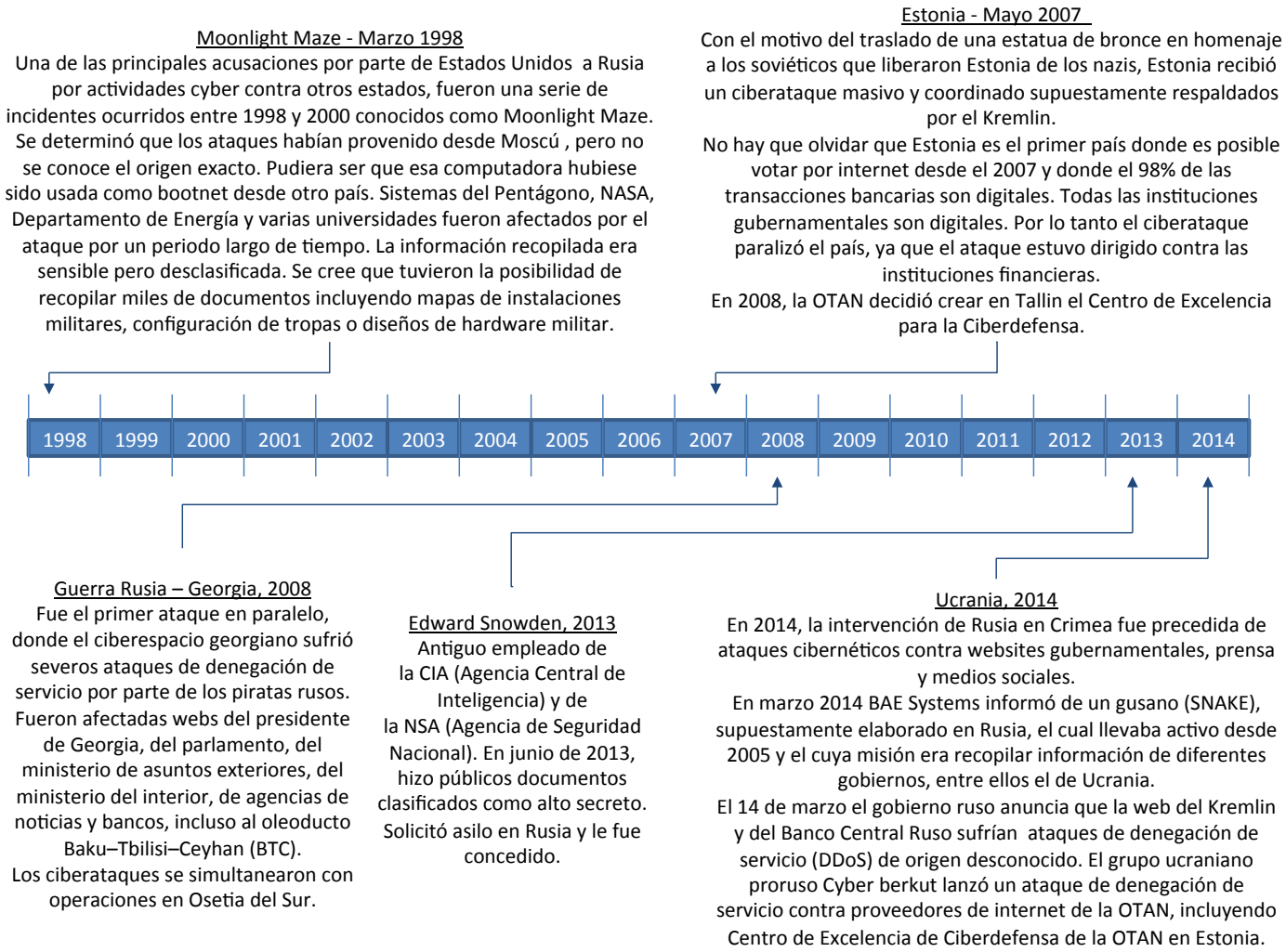
El papel preciso de Rusia en el ámbito del ciberespacio tiene una serie de acciones supuestamente atribuidas como son Cuckoo's Egg, Moonlight Maze, Estonia, guerra Rusia-Georgia, Operación Buckshot Yankee y el caso Edward Snowden entre otros.

Todas estas acciones han contribuido a demostrar la habilidad rusa en esta dimensión, y su apuesta decidida por posicionarse para poder ejercer poder mediante el uso de la información.

La ciber capacidad rusa no reside exclusivamente en las unidades militares, sino también en el crimen organizado o hackers individuales que a cambio de un beneficio crean, venden o distribuyen herramientas ciber. Esta situación se ha dado en conflictos como Georgia o Estonia, y más recientemente Ucrania.

El siguiente artículo es, por tanto, un intento de valorar el poder del ciberespacio a la hora de ejercer poder ya sea como elemento disuasorio, base de influencia, como posicionamiento económico o combinado en una guerra convencional.

ANTECEDENTES



CYBER WARFARE

La guerra Rusia-Georgia, tuvo una serie de ciberataques dirigidos a infraestructuras críticas; se puede considerar como la primera guerra convencional usada como campo de pruebas de una ciberguerra.

De ella se pueden extraer una serie de lecciones aprendidas:

- La evolución tecnológica para controlar el flujo de información debe ir dirigida en tres aspectos:
    - Controlar el tiempo de respuesta.
    - Manipulación de la información.
    - Influenciar.
- El control de la información mediante la ciberguerra habilita a conocer cómo y qué piensa el adversario, sin que este sea consciente de ello y poder ser manipulado o influenciado.

En el ciberespacio es más importante la superioridad en la información que la superioridad tecnológica. El objetivo de la ciberguerra es Controlar y Explotar la información mejor que el adversario.

Estados Unidos, en cuanto a Ciberdefensa, se centra en la protección de las infraestructuras críticas mediante capas de firewalls. También llamadas defensas estáticas.

Se ha demostrado con los diversos antecedentes principalmente rusos y chinos que el enfoque correcto sería redirigirse a defensas dinámicas mediante enrutamiento dinámico, esteganografía y arquitecturas Cloud.

En el año 2000 Rusia publicó su doctrina de seguridad de la información de la Federación Rusa, en ella identificaba tres amenazas:

- Riesgo de conflictos con países fronterizos.
- Confrontación directa con EEUU.
- Conflicto con China

El documento se refiere a la “seguridad informativa” y la utilización de los servicios de seguridad e inteligencia para contrarrestar los esfuerzos hostiles en este ámbito, relacionados con el desarrollo en EE.UU. del concepto de “guerra de la información” o “information warfare” (IW).

En 2010 publicó una nueva doctrina militar, destacando la importancia de la guerra de la información en los inicios de un conflicto, debilitando el mando y el control del adversario, y como campaña de propaganda creando una imagen positiva del conflicto.

Es una declaración del interés ruso por lo que llama el control reflexivo, donde la manipulación y la influencia pasan a primer plano. Y para conseguirlo, se usa el ciberespacio como campo de batalla.

CONTROL REFLEXIVO

La estrategia rusa de control de la información pasa por estar más interesada en los aspectos cognitivos, cuyo objetivo es localizar el eslabón más débil y explotarlo. Son usadas operaciones de desacreditación moral y psicológica (PSYOPS), usando o manipulando datos biográficos, hábitos, deficiencias psicológicas, etc.

La guerra del control reflexivo está comenzando a usarse y quien sea capaz de imitar al contrario, hasta el punto de ***ser capaz de "predecir" su comportamiento***, es el que ganará.

El concepto de control reflexivo está enfocado en Rusia a influenciar en aspectos como la filosofía, sociología, psicología, pedagogía, inteligencia artificial, computación, asuntos militares, inteligencia, contrainteligencia y muchas otras áreas.

INFORMATION TECHNICAL & INFORMATION PSYCHOLOGICAL

En general las teorías militares rusas, separan la information warefare en dos categorías: information-technical y information-psychological, mientras que las definiciones no-rusas, como EEUU o China, usan IW (information warfare) y IO (information operation), incluso a diferencia de Rusia separan en diferentes categorías, psychological operations, computer network operations, operational security o deception.

En un artículo de la revista de la armada Rusa, Morskoy Sbornik en Octubre de 2003, definen la IW en dos partes:

Information-Psychological	Information-Technical
Mass Media	Deception
Internet	Misinformation
Computer network attacks	Radio-electronic intelligence (attack, deception & defense)
Leaflets	Counterintelligence
Religious propaganda	Cryptology
	Steganography

Hay que destacar que Rusia no usa la palabra "cyber", sino que prefiere usar el término "informationization".

Por otro lado Rusia considera que tiene derecho a usar armas nucleares en caso de recibir un ataque cibernético, ya que considera que se ataca a la infraestructura crítica del estado y por lo tanto lo considera legítimo.

Realmente, una respuesta clara a los ataques a Estonia en el 2007, atribuidos a Rusia, fue el establecimiento por parte de la OTAN del Cyber-Security Center en Estonia.

CIBER-CAPACIDADES RUSAS

Organizaciones rusas responsables de las ciber-capacidades ofensivas & defensivas, todas originarias en la KGB:

- FSO (Federal'naya Sluzhba Okhrani o Servicio de Protección Federal). Emplea a cerca de 20.000 personas. La organización supervisa las comunicaciones a alto nivel.
- FSB (Federal'naya Sluzhba Bezopasnosti o Servicio de Seguridad Federal). Formado en el 2003 por 270.000 personas. Su principal función es el cumplimiento de la ley, la seguridad y la contrainteligencia. Su foco es la seguridad del estado.
- GRU (Glavnoye Razvedyvatelnoye Upravleniye o aparato de inteligencia militar). Es la inteligencia militar establecida en 1918. Tiene aproximadamente 26.000 personas en staff. Mantiene unidades de reconocimiento de señales (SINGINT), reconocimiento de imágenes (IMIT), reconocimiento de imágenes por satélite (SATINT) y de inteligencia de fuentes abiertas (OSINT).
- SVR (Sluzhba Vneshney Razvedki o Servicio de Inteligencia Exterior). En 2013 se estima que trabajan 11.800 personas. Es la encargada de proveer información exterior de ayuda a la toma de decisiones, en áreas como política, economía, defensa, ciencia, tecnología y ecología. Sus principales medios son el uso de la inteligencia humana (HUMINT).

COLABORACIÓN

Existen dos características de los supuestos ataques rusos a tener en cuenta:

- Normalmente los ataques rusos, son programados por ellos mismos, no comprados en la Deep Wep. Lo que les hace más propensos a buscar el día cero. Por otro lado la dificultad del idioma ruso, con su alfabeto cirílico le hace de por sí un buen idioma para ser usado en criptografía.
- Además de las poderosas organizaciones gubernamentales rusas, se apoya a los hacktivistas nacionalistas y en la proactividad de los grupos pro-Kremlin (Nashi, jóvenes putinistas...). Esta colaboración público-privada hace imposible la atribución de los ataques. Se da el caso de que los hacktivistas lideran los ataques, el cibercrimen propociona los medios y la Russian Business Network (RBN) vende identidades o servicios de internet ISP. Todo ello con el visto bueno gubernamental siempre que el ataque sea dirigido en función de los intereses de la nación.

CONCLUSIONES

Rusia fue uno de los primeros países que mediante su doctrina de seguridad del 2000, empezó a tener muy en cuenta la capacidad del ciberespacio como la quinta dimensión y poder gestionar cualquier conflicto en ese entorno.

No sólo percibió que la guerra convencional no sería necesaria en la mayoría de los casos, sino que incluso si lo fuera, el uso coordinado de la ciberguerra posicionaría al mejor preparado en la misma.

Como se ha visto en Estonia, Georgia y Ucrania, los ataques desde el ciberespacio le han dado a Rusia una ventaja importante, probablemente por el uso de la ciberguerra en un contexto asimétrico.

Pero el uso que mejor hace Rusia del ciberespacio se enmarca dentro del ámbito de la influencia y la persuasión, ejerciendo poder en base y utilizando la información. Para ello tiene centros especializados en operaciones psicológicas (PSYOPS) para poder influenciar internamente e internacionalmente, y probablemente en muchos aspectos de este tipo puede estar por encima de Estados Unidos.

No hay que olvidar que la autoría de una acción en la mayoría de los casos no se puede demostrar. Además no existe un marco regulatorio común y sobre todo que los costes pueden ser mínimos.

- Se puede realizar un ataque desde un país usando computadoras de otros países (bootnets), e incluso realizando varios saltos para ser más difícil su identificación. Se pueden comprar en la Deep Web claves de tarjetas bancarias, contraseñas de correo o accesos a ciertos sistemas de seguridad.
- Existe una complicación añadida de lo que es ciberdelito y hasta dónde se puede seguir una vez que pasa una frontera de un estado. El ciberespacio puede estar ordenado técnicamente, pero jurídicamente no. Para encausar un delito, se debe proporcionar evidencias electrónicas que tengan validez en los tribunales del mundo físico. Pruebas que evidencien que detrás de un dispositivo específico hay una persona. Además si estamos hablando de ciberataques desde otro país, la cosa se complica aún más. Queda un largo camino que recorrer en este sentido.
- Los costes mínimos y una guerra sin bajas es algo que atrae a los adversarios. Aunque como en el caso de Georgia fue un complemento de la guerra tradicional. Internet garantiza el anonimato y la mayoría de la infraestructura necesaria ha sido invertida (en costes) por el adversario.

El cambio de estrategia derivado de la aparición del ciberespacio como elemento desestabilizador pasa de un sistema resistente a los ataques cuyo objetivo es la invulnerabilidad a un sistema resiliente que sobrevive al ataque, se adapta, sigue funcionando y se recupera cuando el ataque cesa.

Las guerras del futuro se lucharan en el ciberespacio, no mediante ataques de ejércitos tradicionales sino mediante ciberataques, donde un país débil militarmente puede hacer mucho daño con un ataque cibernético.

En cualquier caso, también es cierto que quien más está expuesto a internet, más posibilidades tiene de tener fallos de ciberseguridad.

Como norma, Rusia sólo usa dispositivos creados en su propio país para evitar toda intrusión extranjera mediante virus, o cualquier otro tipo de ciberataque. Esta conciencia de la importancia del ciberespacio es una ventaja sin duda que los países occidentales aún debemos mejorar o mitigar.

"Rusia sólo usa dispositivos creados en su propio país para evitar toda intrusión extranjera mediante virus, o cualquier otro tipo de ciberataque."

El control reflexivo usado por Rusia en cuanto a poder manipular o influenciar al adversario sin que este se de cuenta, es la mayor amenaza, en todos los órdenes, político, militar o económico.

De la misma manera la importancia de los procesos psicológicos (PSYOPS) para proteger su sociedad mediante la televisión, radio o periódicos va dirigida a la estabilidad del estado.

Hay que observar que a día de hoy todos los países desarrollados van evolucionando hacia el Internet de las Cosas (IoT), donde todo está conectado. Por lo tanto el garantizar ataques a Infraestructuras críticas esgrimidas en la Estrategia de Ciberseguridad Nacional deberá ser ampliado a muchos otros dispositivos, así como empezar a dar la importancia que se merece a la concienciación en materia de ciberseguridad.

4 Entrevista a Alvaro Ortigosa.

Director del Centro Nacional de Excelencia en Ciberseguridad (CNEC)

1. A finales de 2012, nace el Centro Nacional de Excelencia en Ciberseguridad (CNEC) que Ud. dirige desde sus inicios, ¿podría resumir los principales logros alcanzados durante estos 3 años?

El CNEC nace hace 3 años con el objetivo de establecerse como referente en formación en temas de ciberseguridad y lucha contra el cibercrimen, con especial énfasis para FCSE. Además, desde el principio tiene una clara vocación de integrarse en iniciativas europeas con otros centros homólogos. En este sentido, los objetivos se han cumplido. Hemos creado un programa de Certificaciones centrado en las necesidades de FCSE, siento pioneros entre los centros europeos en esta iniciativa. De hecho, actualmente participamos de varios proyectos europeos cuyo objetivo es extender el programa actual de certificaciones y establecer marcos comunes de certificaciones en distintos países de la Unión Europea. Para ello colaboramos estrechamente no sólo con otros centros, sino con el ECTEG (European Cybercrime Training and Education Group), un grupo formado principalmente por representantes de los cuerpos policiales europeos y que tiene como objetivo fundamental fomentar y armonizar la formación en ciberseguridad para dichos cuerpos.

2. En la actualidad, ¿cuáles son las principales líneas de trabajo del CNEC?

De los resultados producidos en estos tres años, las certificaciones son el producto más

valorado por los miembros de los FCSE con los que colaboramos. Así que hemos decidido centrar mucho de nuestro esfuerzo en esa línea.

Al mismo tiempo estamos comenzando un programa de máster (Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen) que estamos convencidos tendrá largo recorrido. De nuevo, nuestro objetivo principal con este máster es atender necesidades concretas, tanto de los FCSE como de la sociedad en general. Para ello hemos creado un programa que busca unir la excelencia académica propia de la Universidad Autónoma de Madrid con un enfoque muy práctico, apoyados por numerosos profesionales cuyo día a día consiste en tratar con los temas enseñados en el máster.

3. En su opinión, ¿Cuáles son los principales retos cibernéticos a los que se deberán enfrentar las Fuerzas y Cuerpos de Seguridad del Estado durante los próximos años?

En un futuro cercano preveo que los mayores dolores de cabeza provendrán de los temas que ya están aquí. Por un lado, desde el punto de vista de la defensa, está la preocupación constante por la protección de las infraestructuras críticas. Esta es una preocupación que sólo irá en aumento en los próximo años, al estar estas infraestructuras cada vez más interrelacionados con el factor "ciber" y aparecer más actores con capacidad y, posiblemente, voluntad de atacarlas.

Si consideremos las preocupaciones desde el punto de vista de investigación policial, entiendo que el mayor desafío vendrá por el crecimiento de la computación en la nube, que no sólo creará nuevas vías de vulnerabilidad de los sistemas informáticos sino que le dará una nueva dimensión al problema de recogida de evidencia digital.

Finalmente, el otro factor que ya está aquí es la Internet de las Cosas: por supuesto que es gran marco de oportunidades, que probablemente mejore muchos aspectos de nuestras vidas, pero al mismo tiempo abrimos nuevas puertas que nos hacen más vulnerables, muchas de veces de formas que no llegamos a comprender.

Estos temas sin duda permanecerán a la cabeza de los asuntos a resolver en los, digamos, próximos 4 años. Me es imposible prever qué podremos considerar un reto en el año 2020.

4. En relación a la Estrategia Nacional de Ciberseguridad, ¿piensa que cubre las necesidades de las Fuerzas y Cuerpos de Seguridad del Estado en materia de lucha contra el cibercrimen? ¿En que podría mejorar?

Yo aquí tengo una opinión muy sencilla y concreta: la ENC actual es suficiente. Lo que hace falta es dotarlas de recursos, y que dichos recursos sean utilizados de forma eficiente, evitando, por ejemplo, duplicación innecesaria de esfuerzos. Yo centraría todas las energías en lograr una buena implementación de la ENC.

5. En su opinión, ¿Cómo se podría potenciar el papel de las universidades como actor clave en la ciberseguridad nacional?

La universidad tiene que desarrollar su papel tradicional: formación e investigación de calidad. Pero, especialmente en el tema de ciberseguridad, tiene que hacerlo de la mano de la empresa privada. De esta forma podremos hablar realmente de innovación y se apoyará la creación de tecnología española en ciberseguridad, factor que considero fundamental a la hora de construir una estrategia de ciberseguridad.

Por otra parte, es necesario que la formación en ciberseguridad sea más amplia. Por supuesto, es necesario profundizar los conocimientos de ciberseguridad en aquellas carreras destinadas a formar profesionales involucrados en la creación y adopción de TICs. Pero no sólo aquí: debemos entender que tanto las TICs como lo peligros derivados de su uso permean cada vez más aspectos de nuestras vidas. Es necesario crear consciencia de los riesgos cibernéticos en la medida que afecte a las distintas profesiones y áreas del conocimiento, y la universidad debe ser un pilar fundamental (aunque no el primero) de esta toma de consciencia.

6. Por último, ¿Qué medidas debería implementar nuestro gobierno para fomentar la captación y retención de los jóvenes talentos en el ámbito de la ciberseguridad?

Al respecto estamos convencidos que las labores de captación deben empezar antes de la universidad. Debemos descubrir a los mejores incluso durante la etapa de educación secundaria. Las medidas de captación de talento deberían ir dirigidas en ese sentido.

"Debemos descubrir a los mejores incluso durante la etapa de educación secundaria."

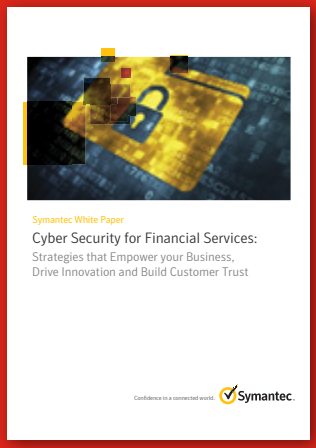
5 Informes y análisis sobre ciberseguridad publicados en diciembre de 2015

2015: el año de las fugas de información (ELEVEN PATHS)

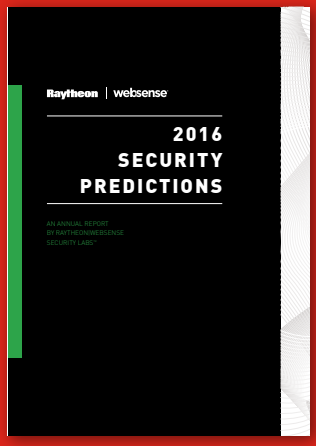
Privacy by Design in Big Data (ENISA)

Latest Report on National and International Cyber Security Exercises (ENISA)

Cybersecurity for Financial Services (Symantec)



2016 Security Predictions (RAYTHEON - WEBSENSE)



European Cyber Security Month 2015 - Deployment Report (ENISA)

2015 Cyber Security Survey: Major Australian Businesses (Australian Government)

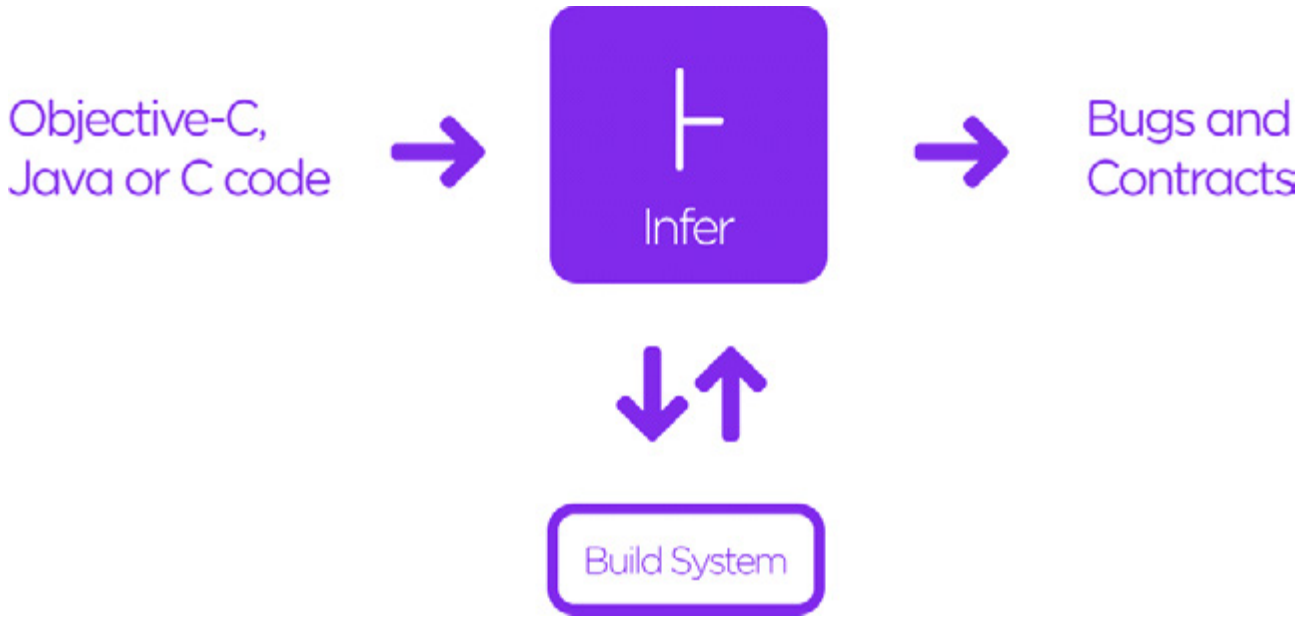
2016 Trend Micro Security Predictions (TREND MICRO)

6 HERRAMIENTAS DEL ANALISTA: Infer

En línea con *Diffy*, presentada en CIBERelcano 7, desarrollada por Twitter, y como continuación a lo acontecido en 2007 cuando liberó *Thrift Technology*, una herramienta usada a nivel interno por la red social para analizar el código fuente en busca de vulnerabilidades, en este caso Facebook presenta una nueva herramienta opensource gratuita llamada Infer.

Facebook Infer es una herramienta de análisis estático de código fuente, de forma que es capaz de analizar código Java o C, produciendo una lista de errores potenciales. Se utiliza parte del proceso de desarrollo de Facebook, ejecutándose sobre los cambios de código para aplicaciones móviles sobre las principales aplicaciones de Facebook para Android e iOS, Facebook Messenger, Instagram y otras aplicaciones que son utilizados por más de mil millones de personas.

Cualquier persona puede utilizar Infer para interceptar errores críticos antes de que hayan enviado a los dispositivos móviles de los usuarios, ayudando de esta forma a prevenir errores de programación y de seguridad.



Entre las principales funcionalidades en entornos Android y Java, Infer informa excepciones de null pointer y pérdida de recursos. Adicionalmente, en entorno iOS, además de lo anterior, se informa de los problemas de pérdida de memoria.

Infer puede ser desplegado localmente e invocado a través de una consola de sistema o bien ser desplegado en entornos de programación o sistemas online como Codeboard.io

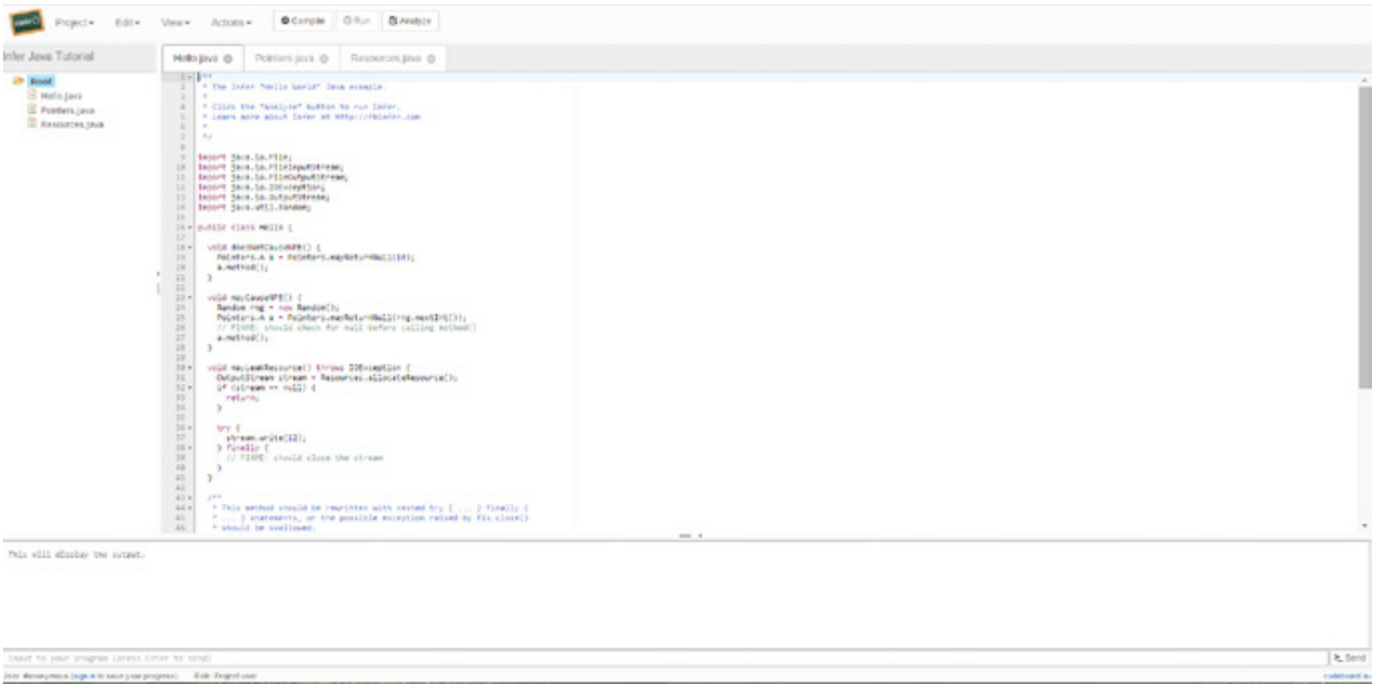


Ilustración 1 Consola web

7 Análisis de los Ciberataques del mes de diciembre de 2015

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

El periodo navideño suele ser muy activo en cuanto a ciberataques, ya que es protagonista de intensas campañas estacionales y de un gran uso de los medios digitales por parte de los usuarios. Una vez más hemos sido testigos de numerosos, pero no por ello extraños, ataques de denegación de servicio y fugas de información de especial relevancia.

CIBERCRIMEN

A principios de diciembre, uno de los órganos más importantes de la anatomía de Internet fue *objeto de un ataque inusual.* En dos ocasiones y durante una hora cada una, se produjo una inundación de peticiones alcanzando picos máximos de hasta cinco millones de consultas por segundo a los servidores DNS raíz que actúan como la referencia final y con autoridad para determinar qué dirección IP se devuelve cuando un usuario escribe un nombre de dominio en un navegador.

El primer ataque se llevó a cabo el lunes 30 de noviembre, y se prolongó durante cerca de 2 horas y 40 minutos. El segundo ocurrió un día más tarde y duró casi exactamente una hora. La mayoría de los trece servidores DNS raíz que forman la zona core de DNS de Internet fueron alcanzados. Los ataques comenzaron y se detuvieron de forma autónoma con millones de peticiones dirigidas sólo a dos nombres de dominio (no revelados), uno en cada ataque. No existen indicios de la autoría del ataque.

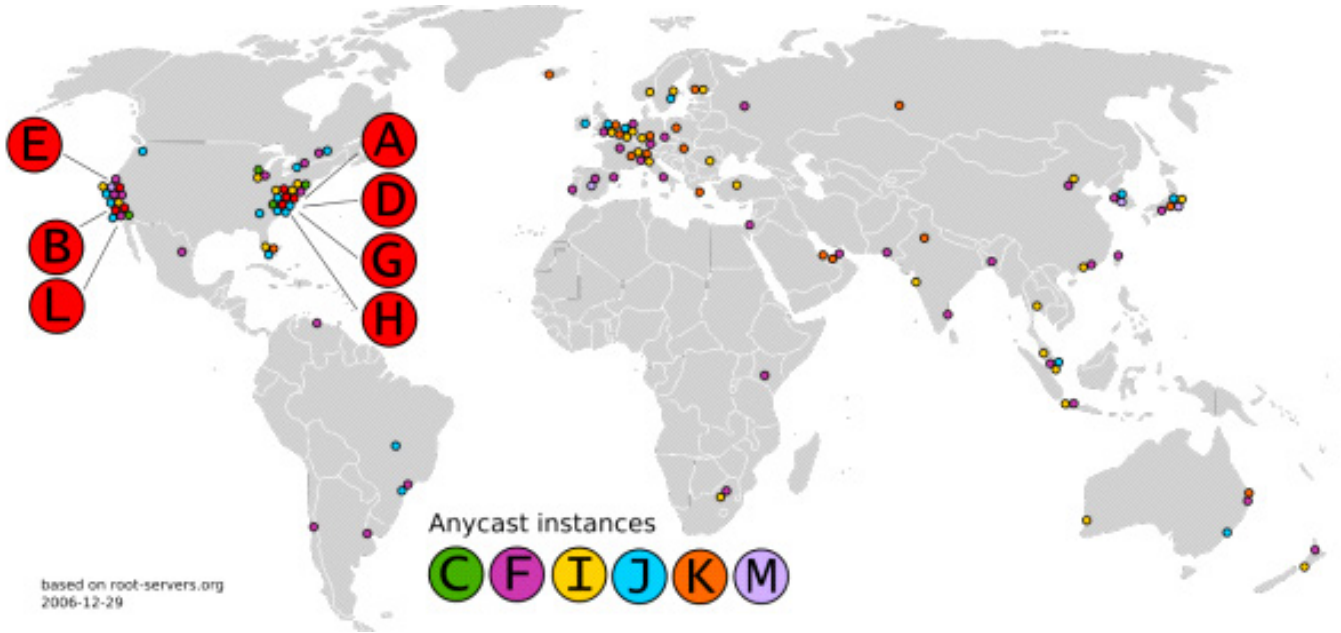


Ilustración 1 Distribución de los servidores DNS raíz

El grupo Phantom Squad, como ya hizo el año pasado por estas fechas Lizard Squad, ha estado a punto de arruinar la Navidad a los jugadores de Microsoft Xbox Live service y Play Station Network, *habiendo lanzado ataques de DDoS*, pero provocando cortes temporales de los servicios desde principios de diciembre.

Phantom Squad, que al parecer obtuvo soporte de otros grupos como VandaSec y Phantoms *también atacaron servidores asociados a otros juegos online* como Star Wars: The Old Republic, Grand Theft Auto 5, Call of Duty: Black Ops 3 y Call of Duty: Black Ops 2.

Ilustración 2 Cuenta de Twitter de Phantom Squad anunciando el ataque

A mediados de diciembre, el Departamento de Seguridad Nacional (DHS) y la (CBP) Agencia de Aduanas y Protección Fronteriza norteamericanas informaron sobre el *ataque realizado por narcotraficantes a sus vehículos aéreos no tripulados* (UAV, drones) para cruzar ilegalmente y en secreto la frontera México-Estados Unidos sin ser observados.

Los drones del CBP son vulnerables a los ataques de suplantación de GPS, el Spoofing GPS es un ataque relativamente trivial, que se basa en el envío a los receptores GPS datos falsos. Cada UAV tiene un receptor GPS, que se utiliza para recibir los datos de los satélites fuera de órbita y navegar a lo largo de la frontera, en busca de personas que cruzan la frontera de forma ilegal. Los narcotraficantes están utilizando técnicas de spoofing GPS para enviar a las UAVs coordenadas falsas, de forma que el UAV corrige el rumbo dejando su área normal de patrulla.

Ilustración 3 UAV del CBP norteamricano usado para control de fronteras

Otro acontecimiento importante en el ámbito del cibercrimen es relativo al descubrimiento de *Packrat*, los investigadores del Citizen Lab, un grupo de vigilancia de Internet con sede en la Universidad de Toronto, publicó un estudio profundo la primera semana de diciembre sobre una campaña de hacking de siete años centrada contra los disidentes políticos, periodistas y otros de América del Sur.

CIBERESPIONAJE

En el plano del ciberespionaje, La unidad 61398 del Ejército Popular de Liberación chino fue acusado a principios de diciembre por *un ataque cibernético importante contra los equipos informáticos de la Oficina Australiana de Meteorología* (bom.gov.au), que ha puesto en peligro sistemas sensibles del Gobierno Federal.

Ilustración 4 Sede de la Unidad 61398, orientada a ciber-acciones ofensivas del Ejército Popular de Liberación chino

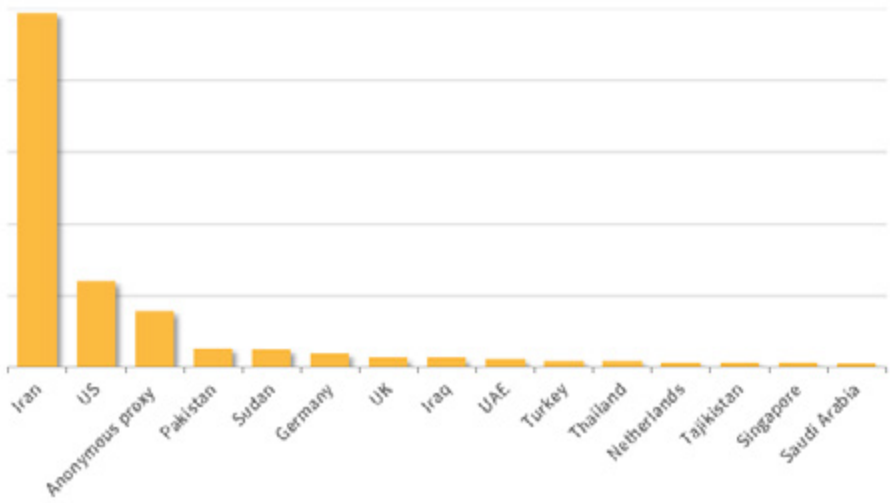


Ilustración 5 Países infectados por los grupos Cadelle y Chafer

Symantec reveló el 8 de diciembre los detalles asociados a dos grupos, muy probablemente con base en Irán, que han llevando a cabo una sofisticada campaña de ciber-vigilancia dirigido a personas y entidades dentro de Irán y en el extranjero desde julio de 2014, y posiblemente desde 2011. Los grupos se han denominado Cadelle y Chafer.

Del mismo modo, investigadores de seguridad de *FireEye desvelaron los detalles sobre APT 16*, un nuevo grupo de APT vinculado a la China continental, focalizado en políticos taiwaneses y miembros de los medios de comunicación, pocas semanas antes de las elecciones en el país.

Juniper Networks emitió un aviso de seguridad urgente el 17 de diciembre debido a un "código no autorizado" que se ha encontrado dentro del sistema operativo utilizado por algunos de los servidores de seguridad de la compañía y en sus firewalls NetScreen. La vulnerabilidad, que puede haber estado activa en algunos de sus servidores desde 2012 y que se incluye en los sistemas de los clientes hasta finales de 2013, permite a un atacante obtener acceso administrativo remoto a los sistemas a través de telnet o de SSH.

HACKTIVISMO

Investigadores de FireEye han identificado una nueva campaña dirigida contra periodistas con base en Hong Kong el pasado 1 de diciembre. La campaña se caracteriza por el uso de Dropbox para albergar la infraestructura comando y control. El grupo, denominado administrador @ 338 se sospecha que está vinculado a China.

Durante este mes, los hacktivistas del colectivo Anonymous han llevado a cabo varias operaciones contra el proveedor de streaming de la Convención de Naciones Unidas sobre el Cambio Climático, Donald Trump, el sitio web del primer ministro de Japón y la Agencia Espacial Europea. En este último caso, atacaron varios subdominios de la página web de la Agencia Espacial Europea provocando la fuga de información personal y credenciales de acceso de más de 8000 suscriptores y funcionarios de la Agencia.

Por otra parte, como reacción a la campaña del Anonymous contra el Daesh #OpISIS (ya comentado en el número 9 de CIBERelcano), el Islamic Cyber Army ha publicado datos personales pertenecientes a funcionarios militares de Francia y Estados Unidos.

Ilustración 6 Captura de pantalla de los datos robados por simpatizantes del DAESH

Durante el mes de diciembre, hemos presenciado otro episodio más del conflicto ciber entre la India y Pakistán. Usando el hashtag #FreeKashmir, un hacker autodenominado *DarkShadow-tn del colectivo AnonCoders ha realizado un defacement de más de 200 sitios web de la India.*

Ilustración 7 Mensaje dejado por DarkShadow-tn en las webs atacadas

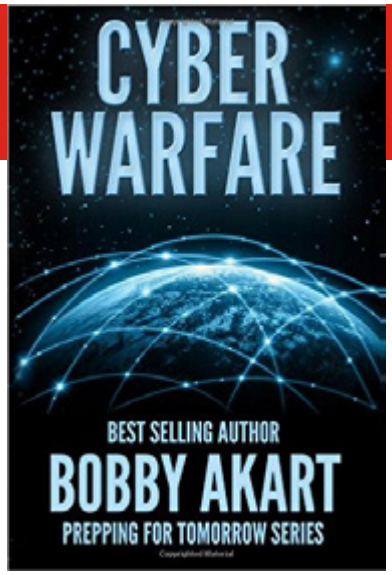
Finalmente, *el gobierno ucraniano ha culpado de los cortes de energía eléctrica en la zona occidental del país a "ataques de hackers de los servicios especiales rusos"*. Según el Servicio de Seguridad de Ucrania (SBU), el malware encontrado en las redes de algunos servicios públicos apuntan a una autoría de Moscú. Por otra parte, estas intrusiones de malware coinciden con una "inundación de llamadas telefónicas en los departamentos de soporte técnico de las plantas de servicios públicos '", según la prensa local.

8 Recomendaciones

8.1 Libros y películas

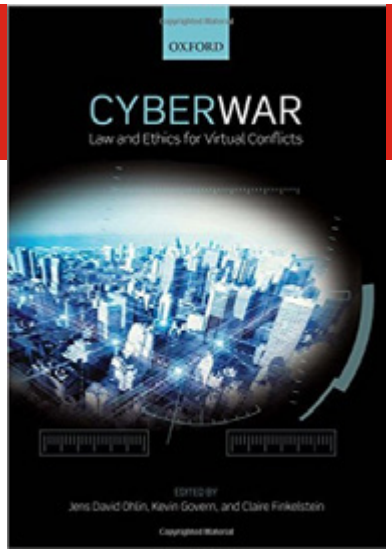
Película:
EL PUENTE DE LOS ESPIAS

Sinopsis: James Donovan, un abogado de Brooklyn (Nueva York) se ve inesperadamente involucrado en la Guerra Fría entre su país y la URSS cuando la mismísima CIA le encarga una difícil misión: negociar la liberación de un piloto estadounidense capturado por la Unión Soviética.



Libro:
CYBER WARFARE: PREPPING FOR TOMORROW

Autor: Bobby Akart
Num. Paginas: 180
Editorial: CreateSpace Independent Publishing Platform
Año: 2015
Precio: 10.00 Euros
Sinopsis: El autor hace una revisión histórica de los principales "actos de guerra" acontecidos en el ciberespacio durante los últimos 50 años, en especial aquellos patrocinados por aactores estatales.



Libro:
CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS

Autor: Jens David Ohlin, Claire Finkelstein y Kevin Govern
Num. Paginas: 320
Editorial: Oxford University Press
Año: 2015
Precio: 25 Euros
Sinopsis: Este libro, escrito por un conjunto de expertos en materia de "ciber-leyes", aborda de manera proactiva los problemas éticos y legales que pudiesen surgir en caso de una guerra cibernética.

Libro:
ZERO DAY: THE THREAT IN CYBERSPACE

Autor: Robert O´Harrow
Num. Paginas: 73
Editorial: Diversion Book
Año: 2014
Precio: 5.00 Euros (e-book)
Sinopsis: Gran parte de la actividad del mundo tiene lugar en Internet. El Pentágono ha declarado que la guerra en el ciberespacio es un hecho inevitable. Durante más de un año, Robert O'Harrow, periodista del Washington Post, ha explorado las amenazas que proliferan en nuestro universo digital, y el resultado de sus investigaciones quedan recogidas en este libro.

Libro:
CYBER WARS: SOCIAL MEDIA IN TIMES OF PEACE

Autor: Hedi Enghelberg
Num. Paginas: 247
Editorial: ENG Publishing
Año: 2015
Precio: 10.00 Euros (e-book)
Sinopsis: El enemigo tiene el mismo talento, hardware y software Lo que hasta hace poco se describía como una guerra totalmente asimétrica (guerras cibernéticas), ahora parece más simétrico que nunca.

8.2 Webs recomendadas

http://agentura.ru/english/
Creado en 2002 por Andrei Soldatov, este sitio web proporciona información sobre las actividades de vigilancia (digital) de los servicios secretos rusos.

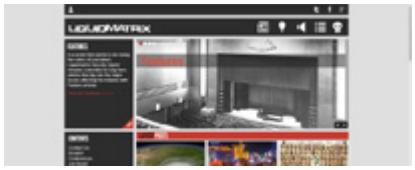
http://usblogs.pwc.com/cybersecurity/
Sitio web de la empresa PWC dedicado a las ultimas tendencias en materia de ciberseguridad.

https://blogs.microsoft.com/cybertrust/
Blog oficial de la empresa Microsoft dedicado a las materias relacionadas con la seguridad en el ciberespacio.

http://blog.noticebored.com/
Gary Hinson proporciona su particular visión de la seguridad de la informacion en NoticeBored.

http://www.hackingarticles.in/
Interesante sitio web creado por Raj Handel donde se comparte información sobre Hacking Ético.

http://www.liquidmatrix.org/blog/
Sitio web que publica análisis propios sobre las principales noticias en materia de ciberseguridad.



8.3 Cuentas de Twitter

@AndreiSoldatov

@buguroo

@Honey_SEC

@YJesus

@virustotal

9 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
2-3 Enero	Las Vegas	AT&T	AT&T 2016 Developer Summit Hackathon	https://devsummit.att.com/hackathon
6-8 enero	Stanford, CA, Estados Unidos	Stanford University	Real World Cryptography Conference 2016	http://www.realworldcrypto.com/rwc2016
14 enero	Singapur	Singapore University of Technology and Design	Singapore Cyber Security R&D Conference (SG-CRC 2016)	http://itrust.sutd.edu.sg/sg-crc-2016/
19-22 enero	Londres	DefenceIQ	Cyber Defence and Network Security 2016	http://www.cdans.org/
21-22 enero	Shangai, China	GRCC	China Automotive Cyber Security Summit 2016	http://www.acss2016.grccinc.com/
25-26 enero	Lille, Francia	FIC	Forum International de la Cybersécurité (FIC 2016)	https://www.forum-fic.com/
26 Enero	Madrid	ICEA	I Congreso sobre Ciberseguridad y Seguros: amenazas y oportunidades en el mundo digital	http://www.icea.es/es-es/formacion/jornadas/Jornadas%20y%20Eventos/2016/I-Congreso-Ciberseguridad-Seguros.aspx?UrlVolver=%2fes-es%2fformacion%2fjornadas%2fpaginas%2fbuscadordejornadas.aspx
25-27 enero	Calgary, Canada	Oil and Gas IQ	Cyber Security for Oil & Gas Canada	http://www.cybersecurityoilgas.com/
26-27 Enero	Tel Aviv	ISRAEL DEFENSE	CyberTech	http://www.cybertechisrael.com/
26-27 Enero	Londres	SINET	The Global Cybersecurity Innovation Summit	http://www.security-innovation.org/global-summit_2016.htm

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