Informe de Amenazas CCN-CERT IA-03/14

Ciberamenazas 2013

y

Tendencias 2014

28 de Marzo de 2014

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad. De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. PRÓLOGO

La sociedad española, su economía, la prestación de servicios por parte de sus Administraciones públicas, la actividad de sus empresas, profesionales y ciudadanos, así como el acceso a la información, la educación, el comercio o el ocio se sustentan hoy más que nunca en el ciberespacio. Trabajar, jugar, comprar, mantener relaciones sociales o financieras o pagar impuestos online, entre otras muchas, constituyen actividades cotidianas que se llevan a cabo usando dispositivos electrónicos y redes de comunicaciones.

Por tanto, para asegurar el mantenimiento de nuestra forma de vida y nuestro desarrollo económico y social, precisamos disponer de un ciberespacio seguro, capaz de conducir nuestras transacciones de manera eficaz y a salvo de ataques o incidentes.

La ciberseguridad, dicho en términos simples, es el conjunto de métodos, procedimientos y herramientas que nos permiten proporcionar seguridad a los sistemas, redes, dispositivos, software y servicios y, por tanto, un requisito previo para que personas, empresas y Administraciones puedan desarrollar su actividad en este entorno. Según recientes estimaciones, el mercado español de la ciberseguridad podría alcanzar cifras cercanas a los mil millones de euros en 2013, estando previsto doblar dicha cantidad en 2017[1].

Sin embargo, la aplicación de la ciberseguridad está lejos de ser simple. Las ciberamenazas son cada vez más numerosas y variadas, tanto que muchas de ellas sufren mutaciones casi a diario.

En la actualidad, las más significativas amenazas a las actividades privadas, empresariales o de la Administración que se desarrollan a través de medios electrónicos, provienen de tres fuentes principales:

1 Pierre Audoin Consultants. "Competitive analysis of the cyber security sector". July, 2013.

Ciberespionaje: recopilación fraudulenta de información con alto valor estratégico, económico, tecnológico, científico o de otro tipo, en poder de los Gobiernos o de empresas, con el fin de obtener una ventaja competitiva o menoscabar la seguridad y el desarrollo nacional.

Ciberdelincuencia: perpetración de acciones delictivas tendentes a cometer fraude y, por lo general, con fines lucrativos.

Hacktivismo: utilización de herramientas digitales con fines políticos[2]. Estas acciones pueden incluir la interrupción de los servicios públicos o las actividades empresariales mediante ataques de denegación de servicio, desfiguración de contenidos o menoscabo de la reputación online de las víctimas.

El número y la sofisticación de las amenazas a nuestros sistemas de información, muy especialmente los gestionados por las Administraciones Públicas y empresas, crecen mes a mes, como así se pone de manifiesto en los diferentes informes que, de forma periódica, publican organismos y empresas especializadas en ciberseguridad, y en el incesante flujo de noticias que, sobre tales materias, publica la prensa diaria.

Un análisis sistemático de los datos generados por la industria de la ciberseguridad de todo el mundo señala que, en 2013, el panorama de las ciberamenazas pasa necesariamente por considerar los siguientes elementos clave:

Ataques dirigidos /APTs	Movilidad
Consumerización / BYOD	Nuevos actores de amenazas
Crime as a Service	Nueva formas de ocultación
Ciberarmas	Ataques contra servicios financieros online
Troyanos para robo de datos	Certificados falsos
Hardware embebido	Ingeniería social
Hacktivismo	Redes sociales
Pérdida de datos de alto perfil	Spam
Sistemas de Control Industrial (SCADA)	SSL y capa de transporte
Legislación y regulación	Ataques contra TSLs
Código dañino	Cloud / Virtualización
Exploits	Normativa interna

Como así se ha señalado en la **Estrategia de Ciberseguridad Nacional**, aprobada el 5 de diciembre del año 2013[3], *la ciberseguridad es fundamental para alcanzar el modelo económico y social perseguido por España, puesto que su adecuado despliegue garantiza nuestra capacidad para asegurar la gobernabilidad y administración del* Estado, *el*

2 Wikipedia: Hacktivismo, acrónimo de hacker y activismo

3 http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D4FEF99D/256935/20131332EstrategiadeCiberseguridadx.pdf

desarrollo de las actividades empresariales o profesionales y el normal desenvolvimiento de la vida privada[4].

Como en sus ediciones anteriores, el objetivo de este documento es describir el marco en el que se movieron aquellos ciberincidentes de 2013 que representaron una amenaza significativa a los intereses de los países, sus organizaciones y sus ciudadanos, incluyendo asimismo un estudio de tendencias para 2014. Con ello, como siempre, además de informar, se pretende concienciar a las instituciones públicas, las empresas y los ciudadanos, de los riesgos que supone operar en el ciberespacio, de forma que sean capaces de tomar las precauciones necesarias y, en su consecuencia, reducir su vulnerabilidad y la de todos.

3. SOBRE EL PRESENTE INFORME

El presente Informe ha sido desarrollado por el Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI). Como se ha dicho, el CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del CCN. Este servicio se creó en el año 2006 como CERT Gubernamental español, y sus funciones están recogidas en el capítulo VII del RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad. Este texto legal, en su artículo 37, señala los servicios que el CCN-CERT ya prestaba desde su constitución (en parte recogidos en el RD 421/2004, de regulación del CCN y en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia).

Así pues, el presente documento es el resultado de la experiencia del CCN-CERT durante 2013 en el desarrollo de sus funciones. Además, se han tenido en cuenta otras fuentes documentales, nacionales e internacionales, contando igualmente con la colaboración de entidades públicas y privadas externas, y profesionales y miembros del mundo académico.

3.1 Contenido

Este documento contiene un análisis, internacional y nacional, de las ciberamenazas y de su evolución prevista, realizado con el propósito de resultar de utilidad para los responsables de la seguridad de las Tecnologías de Información de las organizaciones públicas y privadas de España, así como de sus ciudadanos.

3.2 Ámbito

Se tratan las amenazas detectadas, aunque se ha hecho más énfasis en los países de nuestro entorno occidental. Asimismo, en determinados epígrafes, se han realizado acotaciones específicas para España y los intereses españoles en el extranjero, con especial incidencia en las redes y sistemas de información de las Administraciones Públicas españolas, empresas, profesionales y ciudadanos.

4 Desplegar la ciberseguridad exige disponer de los presupuestos adecuados. A título de ejemplo, diremos que el gobierno del Reino Unido ha destinado, hasta 2016, 860 millones de euros al desarrollo de su Estrategia de Ciberseguridad Nacional.

3.3 Base documental

La información que ha servido de base para la confección del presente Informe proviene de diferentes fuentes: documentos e informes internos del CCN y de sus organismos homólogos internacionales (especialmente, de la UE, EE.UU. y los socios y aliados de España), documentos públicos emanados de las unidades especializadas de los organismos públicos españoles, documentación de terceros -empresas y organizaciones privadas- y, finalmente, estudios y trabajos de profesionales y profesores del sector privado y la Universidad, respectivamente.

A todos ellos les expresamos nuestro agradecimiento.

3.4 Clasificación y periodo de aplicación

El presente Informe se publica con la marca "Sin Clasificar", no estando sujeto, por tanto, a las restricciones relativas a la información clasificada.

Los datos contenidos en el presente Informe comprenden el año natural 2013 incluyendo, en algún caso y para mejor comprensión de la evolución de los hechos citados, algún dato relativo a los meses finales de 2012 y principios de 2014.

La Parte II: Tendencias 2014, contiene algunas de las previsiones que, en las materias citadas, será oportuno esperar de este año en curso.

4. RESUMEN EJECUTIVO

Los incidentes relacionados con la ciberseguridad pueden obedecer a una multiplicidad de **fuentes** y **motivaciones.** Las fuentes, en esencia, pueden dividirse en **externas** (los ataques provienen del exterior de las organizaciones) e **internas** (los ataques provienen del interior de las propias organizaciones). Por su parte, las motivaciones pueden dividirse también en dos grandes grupos: acciones deliberadas (los atacantes actúan con dolo) o accidentales (los atacantes actúan negligente o involuntariamente).

Durante 2013, el grueso de los incidentes, como se muestra en la figura siguiente, ha respondido a acciones generadas desde el exterior de las organizaciones atacadas[5].

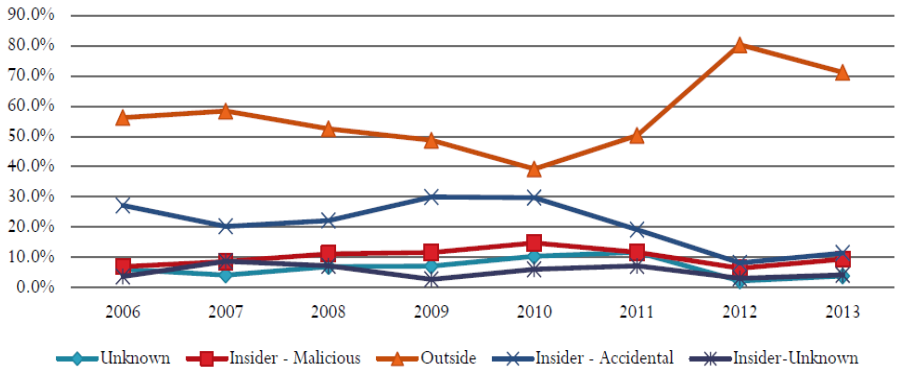


Figura 1. Evolución porcentual de los vectores de ataque durante 2013

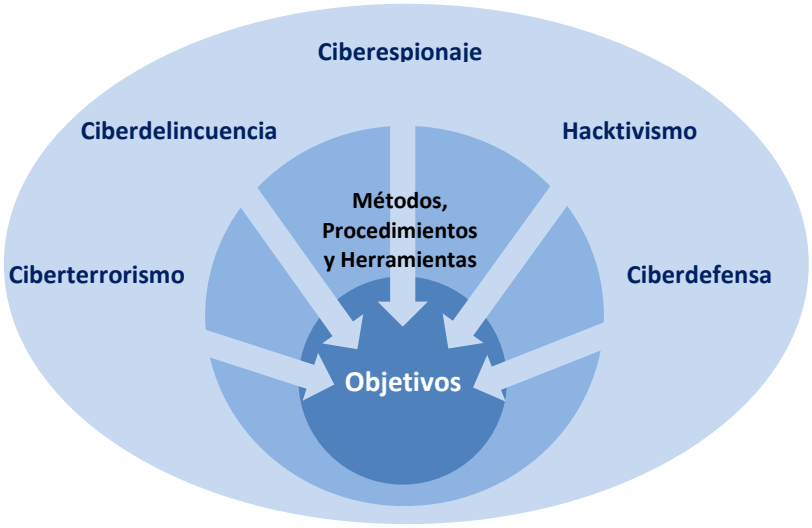
En relación con los ataques externos, la ciberseguridad en 2013 ha girado en torno a los tres ejes fundamentales que han alentado la actividad de los atacantes: **el ciberespionaje, la ciberdelincuencia y el hacktivismo.**

Cada una de estas motivaciones persigue alcanzar sus propios objetivos, de naturaleza política, económica o de cualquier otro tipo, y para ello hacen uso de métodos, procedimientos y herramientas[6].

La figura siguiente muestra un esquema de actores y motivaciones.

5 Fuente: Risk Based Security – Open Security Foundation: Data Breach QuickView (Feb., 2014)

6 En Inglés se conoce por el acrónimo TTP (Tácticas, Técnicas y Procedimientos)



En relación con el **CIBERESPIONAJE** han vuelto a destacar los ataques dirigidos, a través de lo que se ha venido denominando *Advanced Persistent Threats* (**APT**).

Durante 2013 se ha observado un incremento en la sofisticación de este tipo de ataques, sofisticación operativa (circunstancia que se ha puesto de manifiesto al observar cómo los atacantes han comenzado a utilizar rutas de menor resistencia para perpetrar sus acciones) y sofisticación técnica (basándose, esencialmente, en la explotación de vulnerabilidades de día-cero o técnicas personalizadas que se adaptan al modo de actuar de un objetivo concreto).

Estas amenazas, originariamente dirigidas a empresas e instituciones públicas, actúan también sobre personas individuales, incluyendo altos directivos de compañías y de organismos públicos, personajes notorios y responsables políticos.

En 2013 ha destacado la utilización de herramientas de acceso remoto, *Remote Access Tools* (**RAT**), evidenciándose la existencia de canales "comerciales" que han puesto en relación a los creadores de código dañino con sus ejecutores finales.

El número de campañas detectadas por compañías de seguridad se ha incrementado de manera alarmante (Octubre Rojo, grupo APT1, NetTraveler o ICefog).

Por lo que respecta a la **CIBERDELINCUENCIA**, durante 2013 los agentes de las amenazas han incrementado significativamente sus ataques contra Terminales Punto de Venta (**TPV**) y **Cajeros Automáticos**.

La utilización de moneda virtual, como **Bitcoin**, ha constituido en 2013 un elemento de preocupación para las administraciones y los gobiernos de todo el mundo, que se han encontrado con una realidad para la que no existe regulación universalmente aceptada. Muchas empresas y particulares, no obstante, aceptan el uso de este mecanismo de pago.

Finalmente, destaca el empleo de **exploits-kits** por los ciberdelincuentes. A finales de 2013 se detuvo al autor de Blackhole (kit que permitía explotar vulnerabilidades de webs legítimas e infectar a los usuarios que accedían a dichas páginas). En 2014 los diferentes grupos se inclinarán sobre los nuevos conjuntos de herramientas que la sustituyen.

En relación con el **HACKTIVISMO**, este año se ha caracterizado por la aparición de grupos hacktivistas de naturaleza regional, en algunos casos de nueva creación y, en otros, como segregación de *Anonymous*. Es lo que se ha dado en llamar la "balcanización del hacktivismo". Algunos ejemplos significativos han sido los importantes incidentes que han tenido lugar en Brasil.

Por otro lado, en 2013 hemos sido testigos de cómo los Estados han empezado a utilizar las tácticas y procedimientos hacktivistas para desarrollar ataques contra aquellos que, puntualmente, han podido poner en riesgo sus intereses. Quizás, el ejemplo más significativo lo podemos encontrar en la supuesta actuación del grupo hacktivista denominado Anonymous Ukrania, en contra de la incorporación de Ucrania a la OTAN y a la Unión Europea. Otro ejemplo característico es el Ejercito Electrónico Sirio (SEA).

Para completar el panorama de amenazas, no podemos olvidar al **CIBERTERRORISMO** que, aunque con escasa penetración y actividad en la actualidad, persigue provocar terror o miedo generalizado en un grupo o población y, por último, la **CIBERDEFENSA**, que persigue la superioridad en el ciberespacio y que se articula como una nueva misión de las Fuerzas Armadas, contemplando tanto acciones preventivas y defensivas como, en su caso, ofensivas.

Técnicamente existen una serie de **RIESGOS EN CRECIMIENTO**. Así destaca el crecimiento de los ataques usando la técnica del *Watering Hole*, descentralización, DDoS y ataques contra DNS. Todos ellos son examinados en el presente informe.

Además, se analizan los riesgos crecientes derivados de la autenticación de un factor, los ataques contra comunicaciones máquina-a-máquina, las nuevas capacidades de los exploits para eludir los sandbox, las nuevas botnets para plataformas cruzadas, el crecimiento imparable del código dañino para dispositivos móviles, incluyendo el *ransomware* y las nuevas botnes, y el riesgo derivado del creciente uso de los dispositivos móviles (empleo de modelos BYOD), los servicios en la nube (Cloud Computing) y las redes sociales.

El presente informe continúa desarrollando brevemente las **AMENAZAS** más significativas que afectan o pueden afectar a los sistemas de información de las organizaciones, haciendo un repaso de aquellas vulnerabilidades, exploits, código dañino o software potencialmente no deseado, amenazas contra el correo electrónico, sitios web dañinos, dispositivos móviles y bases de datos, que han configurado el panorama general de amenazas durante 2013.

España ha reforzado este año su marco político, normativo y regulatorio en materia de seguridad, empezando por la aprobación, en mayo de 2013, de la **Estrategia de Seguridad Nacional,** documento integrador de todas las políticas que en materia de seguridad desarrollará nuestro país en los próximos años. Una de tales políticas, a semejanza de lo que ha venido sucediendo en otros países de nuestro entorno, ha sido la aprobación también en 2013 de la **ESTRATEGIA DE CIBERSEGURIDAD NACIONAL**, verdadero hilo conductor de la política que en el ciberespacio adoptará nuestro país, sus Administraciones Públicas, sus empresas y sus ciudadanos, para preservar la seguridad de nuestros activos digitales y garantizar la usabilidad de un ciberespacio seguro y confiable.

Durante 2013, además, ha destacado la labor del **CCN-CERT** que llegó a gestionar 7.263 ciberincidentes (un 82% más que el ejercicio anterior) y notificar más de 11.370 vulnerabilidades de hardware y software.

Finalmente, el informe recoge las principales TENDENCIAS para los próximos años y, singularmente, para 2014 desglosadas en nueve grandes grupos: Ciberespionaje y APTs, Código Dañino, Dispositivos Móviles, Servicios de Ciberseguridad, Exploits y Botnets, Ataques contra sistemas operativos y navegadores, ataques de Watering Hole[7] , amenazas del Cloud Computing y Hacktivismo. De todas ellas, destaca una vez más el ciberespionaje y los ataques dirigidos como la mayor amenaza para organizaciones públicas y privadas de todo el mundo, incluyendo el uso de redes sociales y los ataques al "eslabón más débil" (ataques a la cadena de suministro o a los contratistas/proveedores del objetivo final).

El presente documento concluye con unos Anexos que dan cuenta detallada de algunos de los aspectos concretos tratados.

7 En un ataque por Watering Hole, el actor, que quiere atacar a un grupo en particular (organización, sector o región), desarrolla las siguientes acciones: 1.Observa los sitios web que el grupo utiliza frecuentemente. 2. Infecta uno o varios de tales estos sitios web con código dañino. 3. Es bastante probable que algún miembro del grupo objetivo se infectará al acudir a tales sitios. Esta estrategia es muy eficiente, incluso con grupos que son resistentes al spear-phishing.

PARTE I: CIBERAMENAZAS 2013

5. LA EVOLUCIÓN DEL PANORAMA DE LAS CIBERAMENAZAS

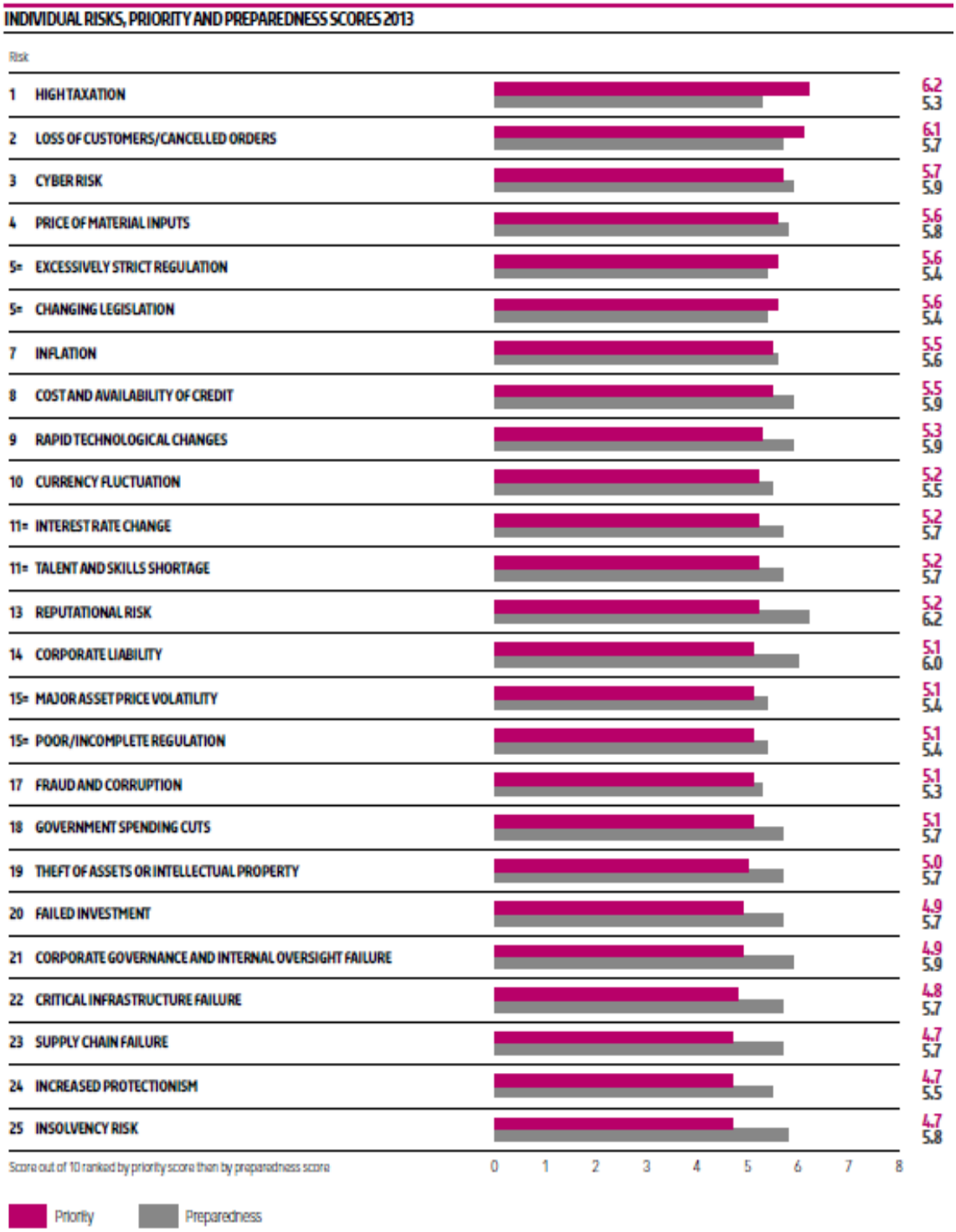
El análisis de los incidentes ocurridos en 2013 ha evidenciado una gran variedad de métodos de ataque, agentes dañinos y víctimas. Durante el pasado año, además de incrementarse las acciones derivadas del ciberespionaje de Estado o corporativo, ha continuado la explotación delictiva de las transacciones online y el desarrollo de actividades hacktivistas. Los agentes de las amenazas (ciberespías, ciberdelincuentes o hacktivistas) han modificado las formas en que se organizan y los métodos seguidos por sus acciones dañinas, todo ello con la pretensión de encontrar nuevos objetivos, asegurar el éxito de sus ataques y eludir la identificación[8].

5.1 Escasa conciencia del riesgo en el ciberespacio

Si tenemos en cuenta la frecuencia –ampliamente documentada- con la que se producen los incidentes, y la importancia que a sus impactos derivados le han venido confiriendo en años anteriores los responsables de instituciones y empresas de todo el mundo, podemos deducir que hasta 2012 se seguían subestimando los riesgos del ciberespacio. El año 2013, sin embargo, ha supuesto un claro punto de inflexión en tal sentido. Según Lloyds[9], el ciberriesgo ha pasado de la duodécima posición que tenían los ataques provocados en 2011, al tercer lugar del ranking mundial de riesgos generales, tal y como se aprecia en la figura siguiente.

8 RSA: "The current state of cybercrime 2013".

9 Lloyd's Risk Index 2013.

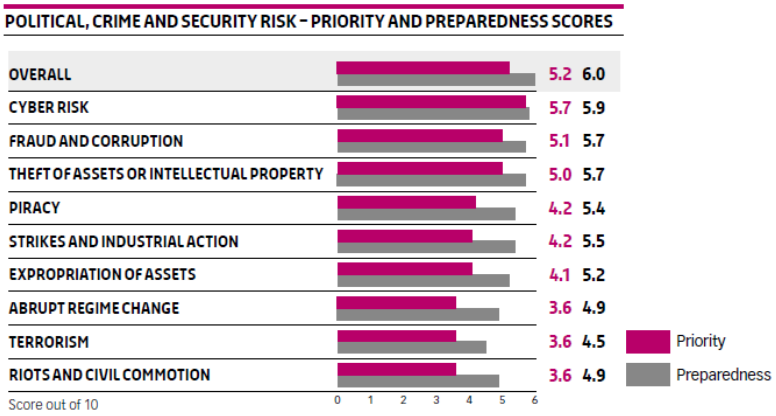


Una de las razones que cabe argumentar para justificar este incremento de la importancia conferida a los ciberriesgos puede deberse al cambio en la percepción que se tiene respecto de los motivos que originan los ataques, que ha evolucionado de la clásica ciberdelincuencia financiera a los ataques políticos, ideológicos y corporativos.

Durante 2013, el número de incidentes atribuidos a los propios Estados ha crecido significativamente. Lo mismo ha sucedido con los ataques generados por grupos hacktivistas, por lo general, como respuesta a acciones gubernamentales.

Un estudio realizado por el Ponemon Institute[10] determinó que el coste medio anual de los ciberataques, tomando como referencia a 56 organizaciones significativas de EE.UU., fue de 8,9 millones de dólares, siendo los ataques más costosos los derivados de APT, los DDoS y los ataques contra páginas web.

Aunque podemos afirmar que las organizaciones de todo el mundo –públicas y privadas- ya están en condiciones de evaluar la realidad de los ciberataques y los riesgos que comportan, parece que, en más ocasiones de lo que sería deseable, su preparación para hacerles frente es escasa. Así, muchas organizaciones creen que son capaces de hacer frente a los riesgos de operar en el ciberespacio, evaluando su "disposición o preparación" para hacer frentes a tales riesgos con una puntuación mayor (5,9) que el propio incremento de los propios riesgos (5,7)[11], tal y como se aprecia en la figura siguiente.



Ranking de Riesgos Generales: Prioridad y Preparación (fuente: Lloyd's)

En nuestro continente, el Comisario para la Agenda Digital para Europa, Neelie Kroes, señaló oportunamente: "*La ciberseguridad es demasiado importante para dejarla al azar o a la buena voluntad de las empresas*". Muchos gobiernos de todo el mundo –España, entre ellos- se han sentido concernidos por esta nueva amenaza y han venido construyendo herramientas y modelos que coadyuven a mitigar los riesgos del ciberespacio[12]. Un ejemplo de ello lo constituyó el acuerdo alcanzado en mayo de 2013 por los senadores republicanos y demócratas para la promulgación de la Deter Cyber Act[13], al objeto de impedir el robo de

10 Ponemon Institute: 2012 Cost of Cyber Crime Study. http://www.ponemon.org/library/2012-cost-of-cyber-crime-study

11 Cifras relativas a EE.UU.

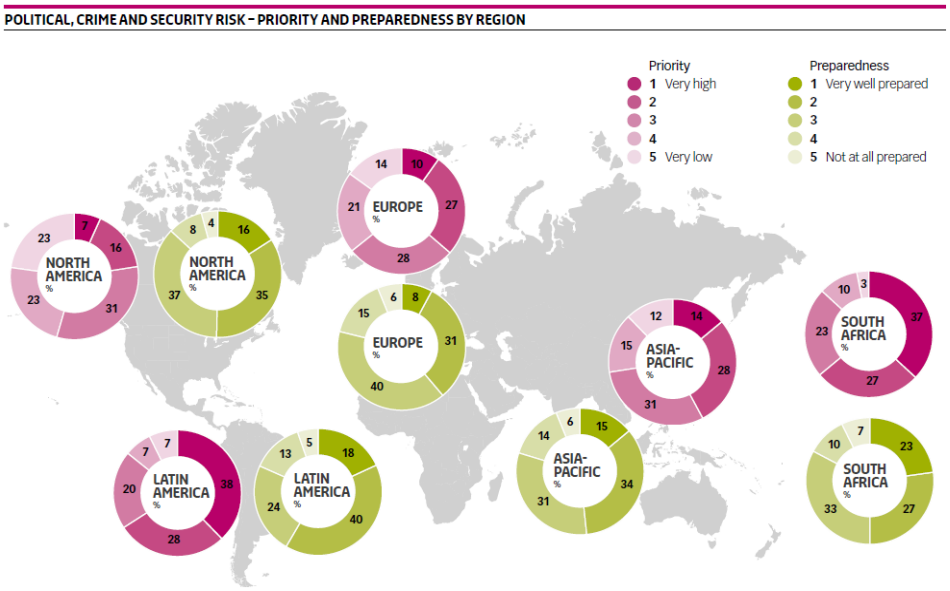
12 En España, en 2013, el paso más significativo lo ha constituido probablemente la publicación de la Estrategia de Ciberseguridad Nacional, cuyos primeros trabajos se iniciaron bajo la dirección del Centro Criptológico Nacional, en 2012, cumpliendo un mandato de la Comisión Delegada del Gobierno para Asuntos de Inteligencia.

13Reuters.http://uk.reuters.com/article/2013/06/06/uk-usacybersecurity-congress-idUKBRE95504H20130606

información comercial de las empresas norteamericanas por parte de empresas y gobiernos extranjeros.

Por su parte, la Comisión Europea está considerando propuestas para exigir a las empresas que almacenan datos en Internet que informen, so pena de las sanciones pertinentes, de la pérdida, robo o puesta en compromiso de información personal.

La figura siguiente muestra el grado de preocupación por los riesgos del ciberespacio y la preparación o disposición para hacerles frente[14].



Finalmente, hay que añadir que una buena parte de los incidentes más frecuentes obedecen a causas que pueden encontrarse dentro de las propias organizaciones. Así, de acuerdo con un informe publicado en abril de 2013 por el Insurance Information Institute[15], la negligencia de los empleados es responsable del 39% de las violaciones de datos y del 24% de los fallos de los sistemas.

5.2 Las tendencias tecnológicas y los riesgos derivados

Atendiendo a recientes estudios[16], dentro del sector IT, en sentido amplio, podemos considerar **cuatro tendencias principales** -e interdependientes- que están redefiniendo el uso de la tecnología, la prestación de servicios por medios electrónicos y, en su consecuencia, las medidas de seguridad a adoptar. Tales tendencias y los riesgos derivados de su uso son:

- Cloud: La posibilidad de usar la red para el cálculo y el almacenamiento de datos, especialmente cuando se trata de nubes públicas o de pago por uso, constituyen elementos paradigmáticos de las nuevas tendencias tecnológicas y su inherente problemática de seguridad.

14 Lloyd's Risk Index 2013.

15 Insurance Information Institute: Cyber Risks: The Growing Threat, 8 April 2013. http://www.iii.org/assets/docs/pdf/paper_CyberRisk_2013.pdf

16 Op. cit. Pierre Audoin Consultants. Julio, 2013.

- Movilidad: El uso de teléfonos inteligentes y dispositivos móviles para acceder a información y realizar transacciones a través de Internet requiere de especiales medidas de seguridad. Destaca el crecimiento exponencial de la conexión de dispositivos móviles a Internet, impulsado por los propios usuarios finales que usan sus dispositivos privados para acceder a las redes corporativas (fenómeno conocido como BYOD, *Bring Your Own Device*).

- Social: El uso de Internet para materializar interacciones sociales –originariamente dirigidas a las relaciones personales o familiares- apuntan ahora, cada vez con más frecuencia, hacia propósitos profesionales, lo que exige medidas de seguridad adicionales.

- Big Data & Analytics: La recolección de grandes cantidades de información y la capacidad de buscar el conocimiento entre los más significativos patrones de comportamiento constituyen acciones que exigen las mayores medidas de seguridad.

Estas cuatro tendencias están impulsando el crecimiento del sector TIC y su relación con la ciberseguridad es innegable. El despliegue de cada una de estas tendencias, como se ha dicho, puede mejorarse si se utiliza dentro de un entorno seguro o empeorarse si se ve afectada por un impacto negativo en la seguridad de la información y de los procesos concernidos.

5.3 Elementos facilitadores de la ciberseguridad en 2013

5.3.1 De la seguridad local tradicional a la ciberseguridad integral

La globalización de las sociedades y sus economías, junto con las tendencias antes mencionadas (universalización de los dispositivos conectados, el cloud computing, la movilidad, etc.) han contribuido a reducir drásticamente la protección que hasta ahora poseían los sistemas de información de las organizaciones.

Antes, los sistemas de seguridad informáticos se concebían como una fortaleza medieval: una enorme protección exterior, pocas puertas y ventanas de reducido tamaño y fuertemente protegidas, lo que proporcionaba al conjunto un escaso y difícil acceso al interior. Desafortunadamente, este enfoque sigue siendo bastante común en muchas empresas e instituciones públicas.

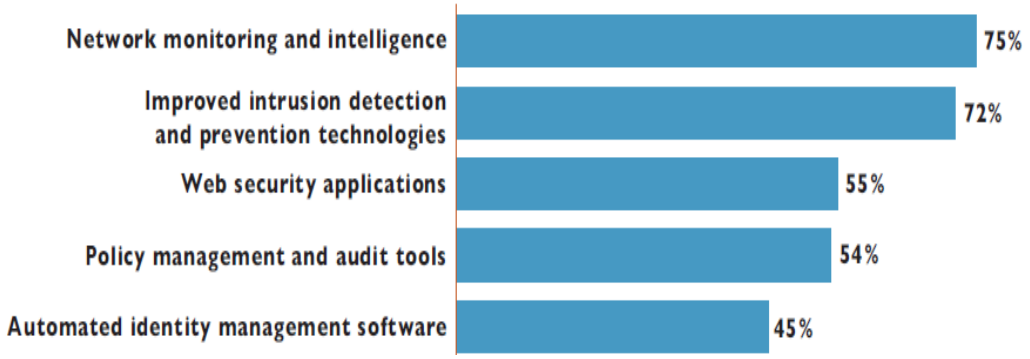
En la actualidad, sin embargo, desde los ordenadores privados a los empresariales, desde los sitios web hasta las infraestructuras consideradas críticas, los sistemas permanecen abiertos al mundo exterior, y así deben continuar, porque así lo demandan los ciudadanos, las empresas y las instituciones públicas y los propios servicios que prestan a todos ellos.

Por todo, las organizaciones están evolucionando desde la concepción local tradicional de la seguridad IT a un enfoque de ciberseguridad integral, más abierto y más complejo[17] donde se fortalecen las capacidades de detección y respuesta adoptando las buenas prácticas de configuración y segmentación. Esta nueva aproximación a la ciberseguridad, si se desarrolla adecuadamente, es compatible con las tendencias derivadas del cloud computing, la movilidad, el big data o las redes sociales.

5.3.2 Tecnologías facilitadoras

Tecnologías tradicionales

Tradicionalmente, se ha considerado que ciertas tecnologías pueden resultar de extraordinaria utilidad para alcanzar la adecuada seguridad de los sistemas de información de las organizaciones. La figura siguiente muestra un gráfico con la importancia concedida a tales tecnologías tradicionales, confeccionada en base a una reciente encuesta llevada a cabo entre los profesionales de la seguridad IT[18] de varias decenas de instituciones en los EE.UU.



Frente a estas debemos considerar aquellas otras que, van haciéndose un hueco entre las herramientas que se emplearan asiduamente en los próximos años. Examinémoslas sumariamente.

Inteligencia y Tecnología Forense

La ciberseguridad es una disciplina en permanente evolución y cambio, por lo que, para ser eficaz, requiere de una constante adaptación. Esta realidad hace que la Inteligencia, el análisis post-incidente y la I+D en materia de ciberseguridad sean actividades de la máxima importancia toda vez que, además de proporcionar conocimiento sobre los ataques sufridos en

17 Para ilustrar esto podemos pensar en dos frutas tropicales: El coco representa el viejo estilo de la seguridad informática como una fortaleza: fuerte por fuera y blando en el interior. El mango representa el nuevo enfoque de la ciberseguridad: accesible desde el exterior aunque con un interior duro. Obviamente, la solución más segura pasaría por una fruta que poseyera una corteza de coco y un núcleo de mango, aunque tal fruta no fuera en modo alguno "comestible", porque no sería rentable ni práctica para la mayoría de las organizaciones, pese a que algunas de ellas, sin embargo, precisarían de ambas protecciones (los servicios de Inteligencia, por ejemplo) para su adecuado desenvolvimiento.

18 Frost&Sullivan 2013 Global Information Security Workforce

el pasado, ayudan a prevenir y contrarrestar nuevos ataques. Todas ellas permiten planificar acciones proactivas, desarrollar mejores prácticas y propiciar la mejora interna de la ciberseguridad de las organizaciones.

Esta inteligencia de seguridad depende de la gestión de vulnerabilidades, la identificación y gestión de los activos, el análisis comportamiento y la capacidad de aprendizaje. Como es lógico suponer precisan, del concurso de equipos de profesionales especializados. Estos equipos desarrollan metodologías y software capaces de analizar los ataques sufridos, generando nuevas y mejores prácticas. Sin embargo, estos son recursos costosos que requieren la combinación adecuada de expertos, investigadores y juristas.

Además de todo ello, se necesita, una infraestructura tecnológica compleja, exigencia que puede satisfacerse a través de acuerdos con operadores de telecomunicaciones o compañías de seguridad gestionada que dispusieren de la tecnología adecuada o disponiendo internamente de Unidades de Inteligencia.

Las Administraciones públicas y entidades como la UE, la OTAN, Interpol, etc., desempeñan también un papel importante en este contexto a través de sus capacidades de respuesta ante incidentes (CERT, *Computer Emergency Response Team*).

Criptografía

En la actualidad, la criptografía permanece en el centro de la seguridad IT y el control sobre su uso sigue siendo fundamental para cualquier país.

La criptografía aplicada a la ciberseguridad se sustenta en algoritmos matemáticos que exigen grandes exigencias de cálculo (tales como la factorización de grandes números), asumiendo precisamente que tal potencia de cálculo es limitada[19].

Los avances en criptografía se han centrado en los últimos años en el uso de ordenadores cuánticos. Aunque todavía está en desarrollo, la computación cuántica permite teóricamente la resolución de algoritmos matemáticos tradicionales mucho más rápidamente. Muchos laboratorios están trabajando en la actualidad en criptografía cuántica aplicada a control de accesos o procesos industriales.

Inteligencia artificial

La Inteligencia Artificial (IA) no tiene la mejor imagen en el mercado TIC generalista, debido quizás a su complejidad y a que muchas de sus primeras promesas no llegaron a cumplirse. Sin embargo, la IA ha encontrado un hueco significativo en ciertos nichos de mercado vinculados a la ciberseguridad (tales como la detección de fraude en tarjetas de crédito)[20].

En ciertos mercados, como la aviación militar o la tecnología espacial, la IA tiene un importante papel, evolucionando desde la mera automatización de plantas industriales hasta

19 Aunque esta premisa está en la actualidad siendo cuestionada, especialmente con la disponibilidad de alta potencia de cálculo a través de modelos cloud.

20 Un ejemplo menos sofisticado pero más popular es la utilización de motores de recomendación, como el usado por Amazon y Netflix ("Usted compró eso, así que pensamos que le gustaría esto otro").

aplicaciones dirigidas a la seguridad, pasando por la robótica. Los primeros sistemas de ciberseguridad que utilizan este tipo de tecnologías han sido algunas soluciones para Defensa y Seguridad, tales como los sistemas de CCTV 911 en Nueva York.

En la actualidad, la IA está ganando terreno gracias a la sofisticación de los ciberataques. Por ejemplo, los modelos de inteligencia artificial podrían detectar anomalías en los sistemas o en el comportamiento de los usuarios, lo que podría evidenciar ciberataques o actividades fraudulentas.

Como es sabido, los sistemas sustentados en IA precisan de una gran potencia de cálculo. Por ello se está empezando a proporcionarse como un servicio en la nube, lo que facilita a los usuarios finales la potencia de cálculo requerida. La computación cuántica se perfila como la próxima generatriz de avance en IA.

Análisis del comportamiento

El Análisis del Comportamiento (*Behavioural Analytics*) presenta dos aspectos:

- Análisis del Comportamiento de la Red: que contempla un análisis del interior de la red, analizando patrones desconocidos, nuevos o inusuales, que podrían indicar una amenaza (detección de anomalías).

- Análisis de Comportamiento Humano: que analiza las interacciones hombre-máquina, contemplando el comportamiento normal de los usuarios. Este método podría identificar, por ejemplo, actividad de código dañino o uso fraudulento de redes sociales[21].

El Análisis del Comportamiento constituye un buen ejemplo de tecnología facilitadora de la ciberseguridad que podría incorporarse a la siguiente generación de tecnología UTM (*Unified Threat Management*) o SIEM (*Security Information and Event Management*). En la actualidad, existen pocos productos comerciales que contemplen estas características.

Gestión de Identidades / Biometría

Los Sistemas de Gestión de Identidades son uno de los principales elementos de cualquier sistema de seguridad. Para los seres humanos, que poseemos la capacidad de reconocer a los individuos de un vistazo, la gestión de identidad puede parecer sencilla. Sin embargo, para los sistemas de información, la tarea de identificar a las personas (sólo unas pocas, o cientos, miles o millones, según las aplicaciones) es una actividad muy compleja.

Los sistemas de Gestión de ID procesan entidades individuales, facilitando su autenticación y ayudando a comprobar sus autorizaciones, roles y privilegios. Entre tales sistemas se encuentran:

- Servicios de directorio.
- Proveedores de identificadores digitales.

21 Obviamente, estos mecanismos deben ser usados conforme a la legislación vigente, respetando los derechos de los ciudadanos y conforme a pautas y normativas previamente conocidas por todos. (Fuente: Prof. Dr. Carlos Galán: "Los componentes jurídicos del análisis del comportamiento". UC3M.

- Soporte electrónico (pasaportes, identificaciones digitales, tarjetas SIM, tarjetas de identificación, etc.)
- Tokens de seguridad.
- Single Sign On.

La gestión de identidades está evolucionando al uso de dispositivos inteligentes (tales como tarjetas inteligentes, tokens, etc.), así como la autenticación por varios factores, combinándose en el futuro inmediato con la identidad basada en notificaciones y los dispositivos biométricos.

En el pasado, la biometría ha tenido que afrontar muchos problemas de índole práctico. Dejando a un lado la resistencia de muchos usuarios a que le sean tomados ciertos tipos de datos como las huellas dactilares o la imagen facial, además, los primeros dispositivos presentaban significativas tasas de falsos negativos que hacían su uso muy incómodo.

Los sistemas biométricos identifican a los seres humanos por sus características físicas. Las huellas digitales ha sido el método más usado. En la actualidad, también se está empezando a generalizarse en determinados entornos el reconocimiento de la retina y el iris e, incluso, técnicas de muestreo de ADN. Además de ello, también es posible identificar a los individuos en base a las señales que producen (como la voz) o patrones de comportamiento (como la dinámica al escribir en un teclado).

5.3.3 Metodologías facilitadoras

Gestión del Riesgo Integral / Identificación y Gestión de Activos

En la actualidad, la gestión del riesgo integral es un catalizador para la ciberseguridad. La normativa reguladora de la industria, de los sistemas financieros o de las Administraciones públicas se encuentra en el núcleo de la exigencia de la implantación de modelos de gestión de los riesgos.

Este enfoque de la ciberseguridad requiere una aproximación multifuncional: el punto de vista del negocio o del servicio, las tecnologías, la ciberseguridad y su implicación económica, así como la exigencia de contar con equipos multidisciplinares preparados para abordar todo ello con garantías de éxito.

La gestión de riesgos y vulnerabilidades, está estrechamente vinculada a la identificación y la gestión de activos y su configuración.

Gestión de Vulnerabilidades

Originariamente, la gestión de vulnerabilidades era una actividad estática que se apoyaba en la auditoría periódica de las defensas de una organización, atendiendo a las amenazas conocidas. Ahora, la gestión de vulnerabilidades debe acomodarse también al impacto de las vulnerabilidades publicadas sobre la infraestructura de la organización.

La gestión de vulnerabilidades se realiza por tres tipos de proveedores:

- Empresas que realizan auditorías de seguridad específicas.
- Vendedores de herramientas, que incluyen tales características en su software.
- Proveedores *SaaS*, a través de servicios en la nube.

En los últimos años, los proveedores SaaS han crecido en número y calidad de prestación de servicios. No obstante, las exigencias –legales– para la custodia de los datos están desafiando la implantación de este modelo, porque el almacenamiento de esta información se realiza fuera de sus propias instalaciones y, en ocasiones, fuera del país.

Seguridad Móvil

El uso masivo de los dispositivos móviles en ambientes profesionales -la movilidad-, está afectando en gran medida la seguridad del entorno-de-usuario (*end-point*). En muchos informes y encuestas, la movilidad se ve como una de las mayores amenazas a la seguridad de los sistemas de información. El advenimiento del BYOD (*Bring Your Own Device*), que representa la fusión de la vida privada con la actividad profesional, tiene profundas implicaciones para la seguridad.

Los actores que están marcando las pautas en la provisión de soluciones para esta problemática son los proveedores de software de Gestión de Dispositivos Móviles (MDM)[22], y los fabricantes de software de seguridad.

Protección de Infraestructuras Estratégicas, Críticas y sistemas SCADA23

El ataque de Stuxnet a las plantas nucleares de Irán en 2010 demostró que las empresas de fabricación, energía y servicios públicos son especialmente vulnerables a los ciberataques, evidenciándose que las amenazas no están simplemente dirigidas a obtener beneficios económicos, sino que también pretenden interrumpir el normal funcionamiento de las infraestructuras atacadas[24].

Los sistemas SCADA, por su parte, plantean una problemática particular: utilizar lenguajes de programación muy específicos, uso de desarrollos software no actualizadas y normalmente mal documentados, o empleo de versiones de software sin soporte y sin configuraciones de seguridad.

Desarrollo seguro por-diseño (by design)

Los responsables de seguridad concentraban sus esfuerzos en la defensa del perímetro y la y la configuración del equipamiento. Ahora, los ataques se dirigen, cada vez con máy la configuración del equipamiento. Ahora, los ataques se dirigen, cada vez con más frecuencia, a las capas de aplicación. Sin embargo, securizar una aplicación que no fue diseñada para ser segura es una tarea muchas veces imposible.

Muchas empresas están empezando a desarrollar aplicaciones seguras "por diseño", comenzando por sus aplicaciones más críticas[25]. Esta práctica ya es obligatoria en

22 Como es sabido, las nuevas características de los sistemas MDM incluyen: protección y borrado seguro de contenidos, sandboxing, administración de parches, cifrado y localización.

23 SCADA: Supervisory Control and Data Acquisition.

24 Las Infraestructuras Estratégicas y Críticas va desde las carreteras a las plantas nucleares, incluyendo el tratamiento de aguas, los aeropuertos, los ferrocarriles, las redes de energía, los servicios de emergencia y las estructuras públicas esenciales.

25 Así concibe el Esquema Nacional de Seguridad de España la seguridad, como un proceso integral que arranca desde el propio diseño de los productos y sistemas.

determinadas industrias, especialmente las que contienen software embebido de carácter científico, técnico o industrial, tal como el que suele utilizarse en sectores como la Defensa, aeroespacial, energía, alta tecnología, telecomunicaciones, entidades financieras o en servicios proporcionados por las Administraciones públicas.

Centros de Operaciones de Seguridad (SOC) / Servicios de Seguridad Gestionada

La gobernanza de la ciberseguridad, generalmente, se gestiona a través de un sistema integrado de ciberseguridad, el SOC (*Security Operation Centre*). Aunque los sistemas SIEM suelen estar en el centro del SOC, estos centros también tienen funciones adicionales:

- Gestión de Activos y vulnerabilidades.
- Inteligencia y Análisis Forense.
- Gestión de Incidentes y Eventos (detección, análisis y tratamiento).
- Servicios de Alertas e informes.

Los SOC posibilitan una mejor gobernanza de la ciberseguridad y un enfoque completo de todas las amenazas. Son útiles para el desarrollo de:

- Auditorías de obligación legal[26].
- Continuidad del negocio y gestión del riesgo.
- Visibilidad de todas las capas de la ciberseguridad.

Los SOC, con frecuencia, se gestionan desde fuera del Departamento TIC de las organizaciones, bajo la supervisión de un Responsable de Seguridad. Obviamente, los SOC también se encuentran en estrecha relación con los departamentos financieros y de asuntos legales de la organización, dada su implicación, especialmente en el caso de existir incidentes de seguridad de carácter grave.

Los SOC, generalmente, requieren mucho personal especializado para la gestión de incidentes y eventos, por lo que también suelen utilizarse SOC desplegados a través de servicios gestionados (vulnerabilidades o de inteligencia de ciberseguridad) aunque nunca en su totalidad.

Servicios de Seguridad Gestionada (MSS)

Como en cualquier modelo de outsourcing, los Servicios de Seguridad Gestionada deben ser cuidadosamente planificados y gestionados para posibilitar una toma de control por personal interno. Para muchas organizaciones de pequeño tamaño, los Servicios de Seguridad Gestionada representan la única posibilidad de alcanzar niveles de seguridad razonables. Muchos de tales servicios se implementarán, además, mediante soluciones en la nube.

En anexo C se muestra la información de este apartado.

26 Tal y como sucede con la auditoría exigida por el Esquema Nacional de Seguridad para los sistemas de información de las Administraciones públicas españolas de determinada categoría de seguridad.

6. LA SEGURIDAD EN EL CIBERESPACIO

6.1 El reconocimiento de las ciberamenazas

Como se verá en epígrafes posteriores, el número de países que han publicado en los últimos años sus Estrategias Nacionales de Ciberseguridad, formalizando con ello su posición frente a las ciberamenazas, evidencia que la ciberseguridad es una preocupación internacional de primera magnitud.

Esta preocupación es especialmente significativa para aquellos países que, como así señalan distintos estudios, sufren importantes brechas y violaciones de seguridad.

La tabla siguiente muestra el "Barómetro de Pérdida de Datos"[27] que la empresa KPMG ha publicado en 2013, comparando las violaciones de datos en distintos países.

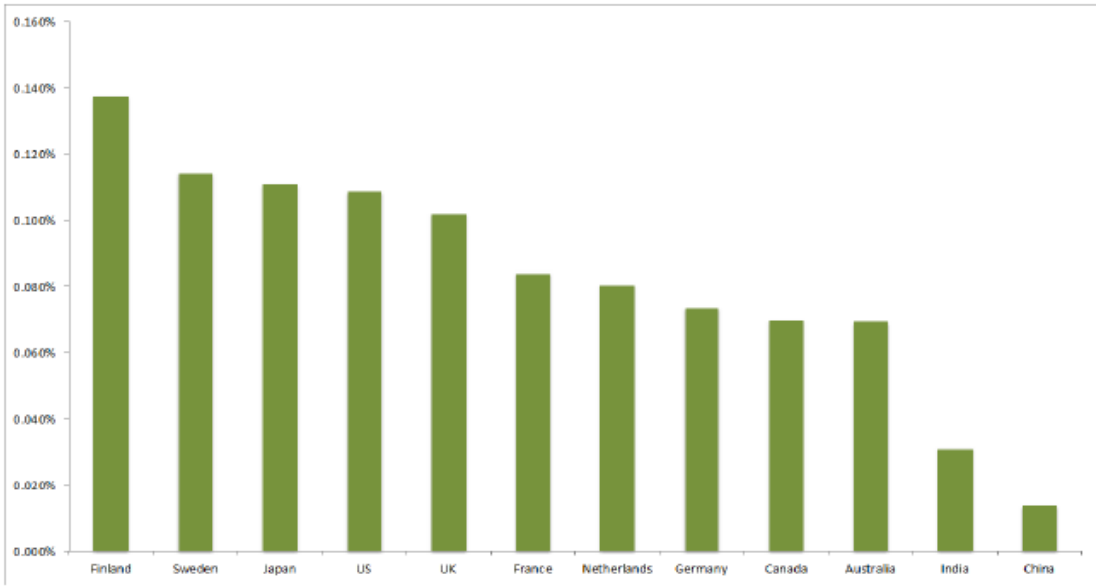
KPMG 'Data Loss Barometer'		
Country	**% Share of Global Breaches 2008-12**	**% Share of Global Breaches 2012**
Australia	1.2	2.0
Canada	3.3	4.2
China	0.5	1.5
India	0.7	2.1
Netherlands	0.5	2.2
UK	**8.4**	**10.1**
US	75.0	47.6
Other	10.5	30.3
		Source: KPMG, 2013

Como se observa en el cuadro anterior, mientras que el porcentaje de las violaciones de datos en EE.UU. ha disminuido de manera significativa, en el resto del mundo se ha incrementado notablemente.

Con las ciberamenazas en franco crecimiento -tanto en frecuencia como en impacto-, parece claro que las respuestas dadas por las diferentes Estrategias Nacionales de Ciberseguridad necesitan igualmente evolucionar. Naciones como Japón, el Reino Unido y los EE.UU. han venido actualizando sus Estrategias de manera continua, respondiendo así a la naturaleza cambiante de estas amenazas. Aunque esta actitud es una señal positiva, también pone de relieve uno de los retos sistémicos de la ciberseguridad: mientras que las ciberamenazas operan dentro de un entorno fluido y en permanente cambio, las Estrategias Nacionales de Ciberseguridad son, por definición, documentos estáticos, aunque su contenido se actualice periódicamente.

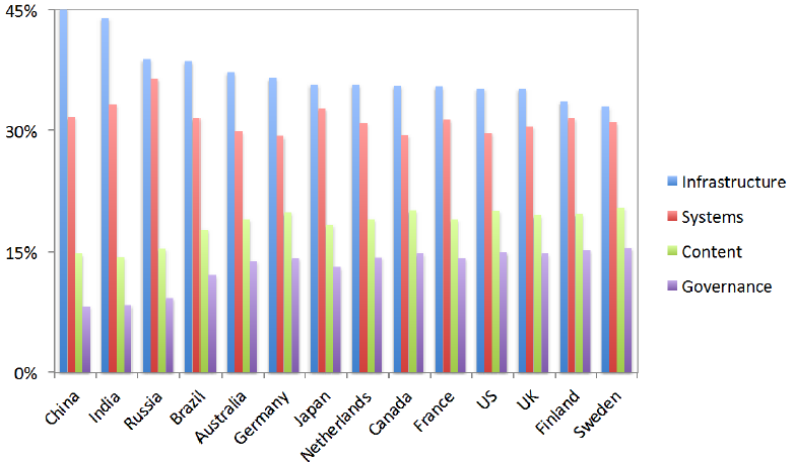
A efectos de valorar el compromiso de diferentes países, la figura siguiente muestra los gastos en ciberseguridad en relación con su Producto Interior Bruto. Obsérvese que, proporcionalmente al PIB, las inversiones en ciberseguridad de los EE.UU. están por detrás de los realizados por países como Finlandia, Japón o Suecia.

27 KPMG. "Data Loss Barometer" 2012.



Inversiones en ciberseguridad de diferentes países como porcentaje del PIB[28]

Una medida de la madurez en el enfoque de las inversiones en ciberseguridad es examinar tales inversiones por sectores. La regla general es que los sectores más maduros en seguridad IT invierten proporcionalmente menos en infraestructura y sistemas y más en gobernabilidad y contenidos. En los sectores menos maduros, se invierte esta regla. Esta posición se ve confirmada por las cifras que se muestran en la figura siguiente.



Inversiones en ciberseguridad por países y sectores

6.2 Los ciberataques de 2013

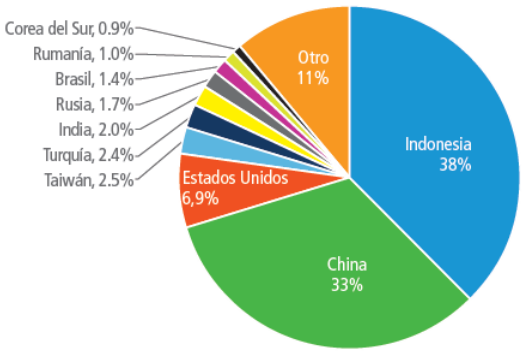
28 Fuente: Pierre Audoin Consultants. "Competitive anáylisis of the UK cyber security sector" (Jul, 2013)

6.2.1 Tráfico de ataque y orígenes

Según los análisis realizados por distintas compañías[29], en 2013 se observó un tráfico trimestral de ciberataques cuyo origen se sitúa, esencialmente, en 175 países o regiones distintas.

Como se observa en la figura siguiente, Indonesia y China compartieron el liderazgo de los ciberataques en el segundo trimestre de 2013, manteniéndose los EE.UU. en tercer lugar, lo que representa un poco menos del 7 % de los ataques observados. Como puede observarse en la figura, la región de Asia/Pacífico fue responsable de poco más de 79% de los ataques observados. Europa representó algo más del 10%, mientras que América (Norte y Sur) también representó poco más del 10 %. La contribución de África siguió disminuyendo en 2013, toda vez sólo le es imputable un tres por mil de los ataques.

	País	% de tráfico 2T13	% 1T13
1	Indonesia	38%	21%
2	China	33%	34%
3	Estados Unidos	6,9%	8,3%
4	Taiwán	2,5%	2,5%
5	Turquía	2,4%	4,5%
6	India	2,0%	2,6%
7	Rusia	1,7%	2,7%
8	Brasil	1,4%	2,2%
9	Rumanía	1,0%	2,0%
10	Corea del Sur	0,9%	1,4%
–	Other	11%	18%



Tráfico de ataque. Principales países originarios (atendiendo a su dirección IP)

6.2.2 Puertos atacados

Como se muestra en la figura siguiente, la concentración de los ataques a los 10 principales puertos elegidos como objetivo aumentó en 2013 en un 82%, concentrándose los ataques a los puertos 80 (WWW/HTTP), 443 (SSL/ HTTPS) y 445 (Microsoft-DS)[30].

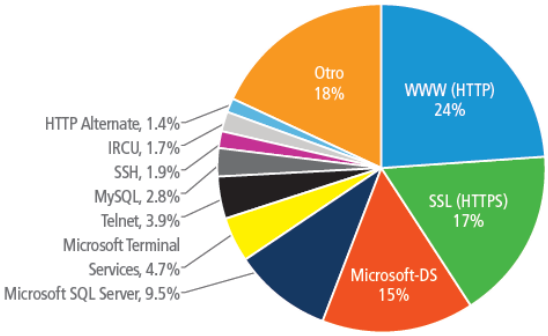
También aumentaron los ataques contra los puertos 1433 (Microsoft SQL Server), 3306 (MySQL), 6666 (UCRI) y 8080 (HTTP Alternate). Sin embargo, se observó un descenso de los ataques contra los puertos 445, 3389 (Microsoft Terminal Services), 23 (Telnet) y 22 (SSH).

El puerto 445 sigue siendo el objetivo principal en siete de los 10 países. Por su parte, el puerto 1433 (Microsoft SQL Server) permanece como el principal blanco de los ataques originados de China. El puerto 6666 (IRCU) también fue objeto de ataques provenientes de China (cuarto puerto más atacado). Por su parte, el puerto 23 (Telnet) siguió siendo el principal blanco de los ataques originados en Turquía.

29 Los siguientes datos provienen de Akamai: "El estado de Internet" (Vol. 6, núm. 2; 2013), recogidos de su plataforma inteligente distribuida por todo el mundo

30 El 90% de los ataques dirigidos a los puertos 80 y 443 se originaron en Indonesia en el segundo Trimestre de 2013 (Fuente: Akamai).

Puerto	Uso del puerto	% de tráfico 2T13	% 1T13
80	WWW (HTTP)	24%	14%
443	SSL (HTTPS)	17%	11%
445	Microsoft-DS	15%	23%
1433	Microsoft SQL Server	9,5%	8,3%
3389	Microsoft Terminal Services	4,7%	5,4%
23	Telnet	3,9%	9,3%
3306	MySQL	2,8%	2,7%
22	SSH	1,9%	2,6%
6666	IRCU (IRC Undernet Daemon)	1,7%	1,2%
8080	HTTP Alternate	1,4%	1,5%
Varios	Otro	18%	–



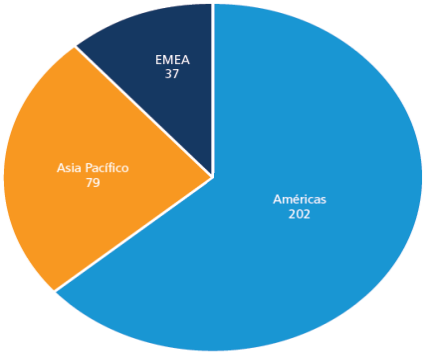
Tráfico de ataque. Puertos atacados.

6.2.3 Observaciones sobre los ataques DDoS

Durante 2013 hemos visto que los agentes de las amenazas que llevan a cabo ataques de Denegación de Servicio Distribuida (DDoS) se están esforzando cada vez más para que sus ataques parezcan "*flash mobs*" legítimos, intentado con ello eludir las medidas de seguridad.

Según datos de la compañía Akamai, ha proseguido el aumento en el número de ataques notificados trimestralmente. Aunque se informaron un total de 768 ataques en 2012, en el primer semestre de 2013 esta compañía recibió 516 informes de ataque. En el segundo trimestre de 2013 fueron 318 informes de ataques. Algunos de estos ataques fueron atribuidos a la guerrilla izz ad -Dim al-Qassam Cyber Fighters (QCF).

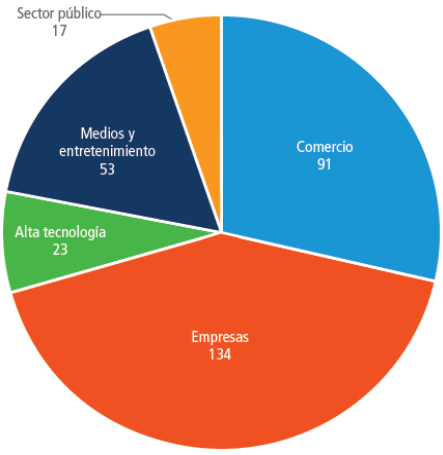
Si bien el continente americano representó casi dos tercios de todos los ataques, tal como ilustra la figura siguiente, se produjo un cambio significativo de los ataques en Europa, Oriente Medio y África a la región de Asia Pacífico. Así, el número de ataques en Asia casi se triplicó en el segundo trimestre, subiendo hasta 79 frente a los 27 observados en el primer trimestre. Europa fue la única región que experimentó una disminución en los ataques, bajando de 47 ataques en el primer trimestre a 37 en el segundo trimestre. El aumento de los ataques en Asia se vio impulsado principalmente por una serie de ataques a un pequeño número de empresas de la región.



Ataques DDoS por región (2T2013)

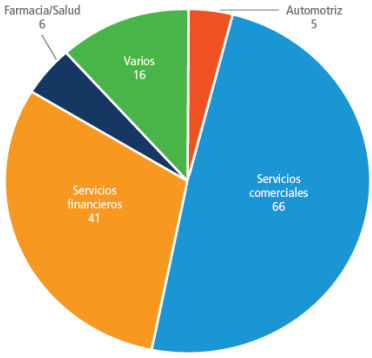
Según las mismas fuentes, y tal y como se muestra en la figura siguiente, el sector "Empresas" continuó siendo el blanco principal de los ataques DDoS, seguido por "Comercio" y "Medios y entretenimiento", en segundo y tercer lugar, respectivamente. El sector "Empresas" registró el aumento trimestral más significativo, pasando de 72 ataques en el primer trimestre a 134 en el segundo. "Comercio" también registró un aumento significativo: de 67 a 91, aunque

"Medios y entretenimiento" experimentó un crecimiento relativamente pequeño: de 45 ataques a 53. Por su parte, el número de ataques dirigidos contra el "Sector Público" y "Alta tecnología" también continuó creciendo.



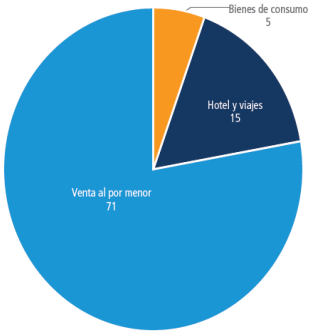
Ataques DDoS por sector (2T2013)

La figura siguiente muestra la distribución de ataques por sectores empresariales.



Ataques DDoS por sector empresarial (2T2013)

La figura siguiente muestra la distribución de ataques, dentro del sector "Comercio".



Ataques DDoS en el sector del comercio (2T2013)

Finalmente, el sector "Medios y entretenimiento" experimentó un crecimiento relativamente mínimo en el número de ataques DDoS, en comparación con el número total de ataque DDoS. Casi todos los ataques en este sector durante el segundo trimestre se

dirigieron contra las compañías de medios de comunicación, registrándose un sólo ataque contra una compañía de juegos, en comparación con los cuatro del primer trimestre.

6.2.4 Los ataques del Ejército Electrónico Sirio

Durante el segundo trimestre de 2013, un grupo autodenominado Ejército Electrónico Sirio (Syrian Electronic Army - SEA) reivindicó varios ataques de alto perfil contra empresas periodísticas y medios de comunicación[31]. Los ataques fueron diseñados para difundir propaganda a favor del régimen del presidente sirio Bashar al-Assad.

Uno de los ataques más notables atribuidos al SEA fue contra la Associated Press, en Twitter. Tras difundirse una falsa sobre un atentado en la Casa Blanca, se produjo una caída de 150 puntos del Dow Jones Industrial Average (DJIA), debido a que los sistemas automáticos de valoración reaccionaron a la falsa historia y procedieron a vender activos de forma masiva. Esta caída hizo que el Dow Jones perdiese 140 mil millones de dólares -el 1% de su valor- en tan sólo 90 segundos[32].

Desde entonces, se le han atribuido al SEA ataques contra otros medios de comunicación, tales como The Guardian, The Financial Times o The Onion. En cada uno de estos ataques, las tácticas empleadas fueron muy similares: el atacante lanzó un ataque de phishing contra el objetivo, comprometiendo, al menos, una cuenta de correo electrónico interna. Utilizando esas cuentas, se lanzaron nuevos ataques, hasta que los atacantes recopilaron las credenciales que proporcionan acceso a Twitter, transmisiones RSS u otra información sensible.

En todos los casos, el SEA parecía interesado en diseminar propaganda pro siria, aprovechando la audiencia de las transmisiones en los medios sociales más populares. También se ha asociado este grupo con la publicación de propaganda pro-siria en las páginas de Facebook, de la Embajada de EE.UU. en Damasco, del Departamento de Estado de EE.UU., del Departamento del Tesoro de EE.UU., de Hillary Clinton, de Brad Pitt, de Oprah Winfrey, de la ABC News, de la Casa Blanca, y del presidente Barack Obama. Hasta la fecha, la organización, además, ha preferido atacar objetivos que han apoyado públicamente a los rebeldes sirios en vez de llevar a cabo desfiguraciones de sitios web o exfiltración de datos.

Como se ha dicho, los ataques del SEA comenzaron principalmente a través de ingeniería social, por lo general a través de ataques de phishing. Es difícil cualquier relación entre el SEA y el gobierno sirio que, no obstante, aprueba sus acciones. El Presidente al-Assad señaló en un discurso en junio: "El ejército se compone de los hermanos de cada ciudadano sirio, y el ejército siempre es sinónimo de honor y dignidad. Los jóvenes tienen un importante papel que desempeñar en esta etapa, ya que han demostrado ser una potencia activa… Existe el ejército electrónico que ha sido un verdadero ejército en la realidad virtual"[33].

31 http://blogs.wsj.com/corporate-intelligence/2013/04/30/what-you-need-to-know-about-the-syrian-electronic-army/

32 http://www.cbc.ca/news/technology/who-is-the-dow-jones-wrecking-syrian-electronic-army-a-hacker-explains-1.1330203

33 http://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background

Finalmente, también se atribuyó al SEA los ataques del tercer trimestre de 2013 contra la infraestructura DNS de algunos dominios del New York Times, el Huffington Post y Twitter.

6.3 Los riesgos más significativos

6.3.1 El ciberespionaje

Como es sabido, se viene denominando ciberespionaje a aquel tipo de ciberataque perpetrado para obtener, esencialmente: secretos o información sensible de Estados; propiedad intelectual o industrial de organizaciones públicas o privadas; información comercial, financiera o empresarial sensible o relevante; o datos de carácter personal de personalidades, personajes públicos o notorios y, en general, de cualquier persona y que puedan ser usados como medios para alcanzar objetivos finales.

Durante 2013, el volumen de informes públicos asociados con el ciberespionaje o con su vector de ataque más relevante -las APTs[34]-, aumentó significativamente. Tales informes muestran no sólo las herramientas e infraestructuras que estos grupos vienen utilizando, sino también, en algunos casos, a sus responsables directos[35]. Mandiant Corporation inició el año apuntando específicamente a la Unidad 61.398 del Ejército de Liberación del Pueblo, de la República Popular China. En respuesta a estos informes públicos, los atacantes cambiaron sus tácticas y mejoraron su seguridad operativa.

La figura siguiente muestra la dispersión geográfica de los ataques por APT más significativos durante el pasado año. El tono de color de cada círculo representa el volumen de los ataques en el país considerado.

34 Advanced Persistent Threats – Amenazas Persistentes Avanzadas.

35 Véase, por ejemplo: "APT1: Exposing One of China's Cyber Espionage Units." Accessed on Dec. 18, 2013. Mandiant. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

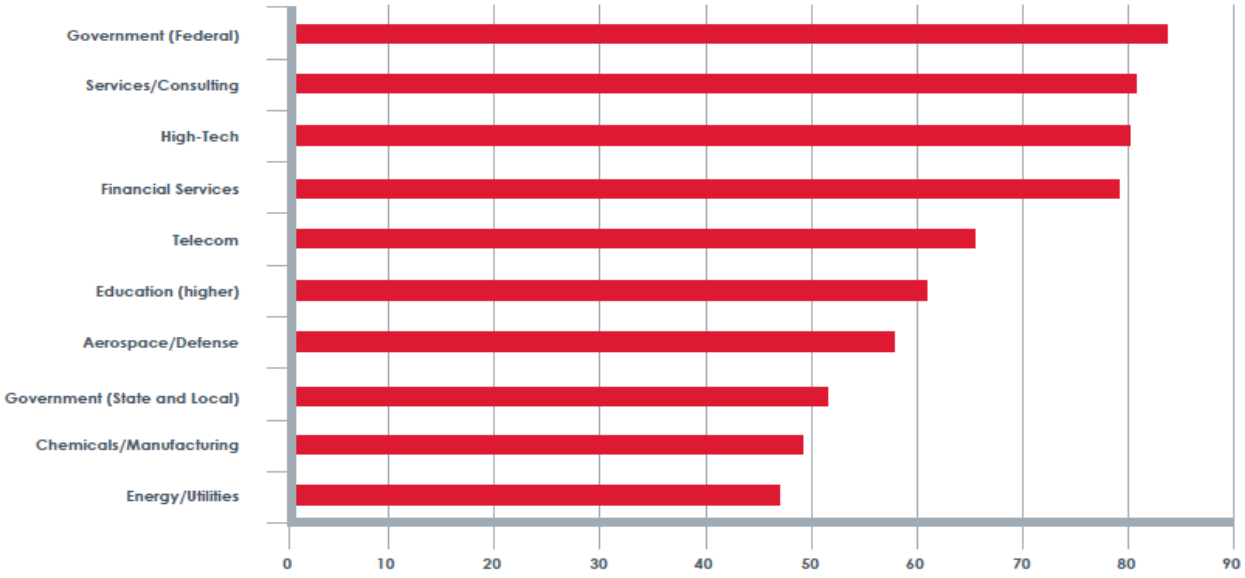
Atendiendo a los datos manejados por FireEye[64], los 10 países más atacados han sido: Estados Unidos, Corea del Sur, Canadá, Japón, Reino Unido, Alemania, Suiza, Taiwán, Arabia Saudita e Israel.

El ejemplo de Mandiant no es un caso aislado. En 2013, las empresas de seguridad no sólo informaron a la opinión pública de los ataques APT de los que se tenía noticia, sino que también hicieron un esfuerzo por interrumpir estas operaciones, recopilando la mayor cantidad posible de información sobre sus orígenes y métodos antes de publicarla. Este comportamiento provocó cambios en la seguridad de operación de estos grupos. Así, por ejemplo, los actores chinos de la llamada APT1 redujeron drásticamente sus operaciones contra cualquier objetivo nuevo o ya existente, observándose que se abandonaban muchos de los servidores C&C que habían sido usados con anterioridad.

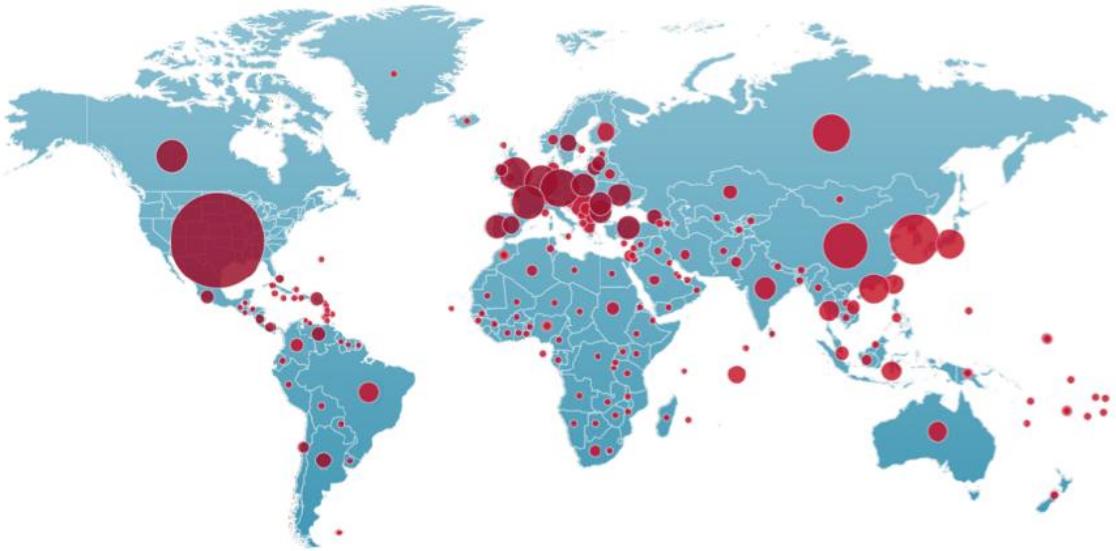
Cuatro meses después del informe de Mandiant, la empresa Kaspersky publicó un informe con las operaciones del grupo de APT denominado NetTraveler[36]. De manera similar a lo que había sucedido con APT1, los actores que participaban en las operaciones de NetTraveler hicieron un rápido ajuste de sus operaciones, abandonando los anteriores servidores y herramientas, para empezar a utilizar un mayor abanico de instrumentos de ataque. Sin embargo, en este caso, las acciones no detuvieron en ningún momento.

Si algo se ha evidenciado 2013 es que los ataques APT han escogido cuidadosamente sus objetivos, públicos y privados. Según el antedicho informe, el mayor número de ataques por malware específico los han sufrido los siguientes sectores: Gobierno (Administraciones Públicas), Servicios y consultoría, Tecnología, Servicios financieros, Telecomunicaciones, Educación, Aeroespacial y Defensa, Química y Energía. La figura siguiente muestra el número de familias de código dañino usado en los ataques APT, por sector atacado.

36 "The NetTraveler (AKA 'TravNet')". Último acceso: 20.12.2013. Securelist.
http://www.securelist.com/en/downloads/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf



La figura siguiente muestra la distribución geográfica respecto de la localización de los sistemas de Mando y Control (C&C) usados en las fases iniciales de los ataques tipo APT en 2013.



Por otro lado, en 2013, existen evidencias que en algunos casos, una vez que estos habían infectado los sistemas de las víctimas los atacantes, limpiaban su código dañino y salían del sistema atacado si no cumplía éste ciertas condiciones. Este comportamiento demuestra un nivel de madurez y capacidad de selección de objetivos muy elevado.

El cuadro siguiente muestra las que han constituido en 2013 fuentes principales de este tipo de acciones, cuando han sido patrocinadas por los propios Estados.

Rusia:	○ Mediante la utilización de herramientas específicamente diseñadas para actuar contra los objetivos previamente seleccionados. ○ Poseyendo un conocimiento técnico muy elevado. ○ Ataques dirigidos contra las AA.PP. y sectores estratégicos específicos ○ 432 incidentes en 2013, 9 de ellos de naturaleza crítica.
China:	○ Con un programa activo desde 2001. ○ Interés específico en la propiedad Intelectual de los siguientes sectores empresariales: aeroespacial, energía, defensa, gubernamental, farmacéutico, químico, tecnologías de la información, financiero y transporte. ○ Usando (en muchos casos) herramientas comerciales. ○ Existen diferentes grupos que poseen un perfil técnico muy variado. ○ 477 incidentes en 2013. 11 de ellos de naturaleza crítica.
Otros Países	○ Revelaciones de Snowden. ○ Adquisición de herramientas de ataque comerciales puestas a disposición de los diferentes gobiernos.

El cuadro siguiente muestra las cuatro APT más significativas de 2013, incluyendo fechas de sus acciones, tipología de víctimas, origen atribuido y fecha de detección.

Octubre Rojo:	• Enero 2013 • Agencias gubernamentales / diplomáticas • Empresa sector aeroespacial y energéticos (Industria Nuclear) • Interés en Herramientas cifra OTAN / UE • Posible origen RUSIA • Detectado: Octubre 2012. KASPERSKY
APT1:	• Febrero 2013. Unidad 61398. Shanghai. 2000 personas. • Persistencia: 356 días (Max 4 años y 10 meses) • Posible Origen CHINA • 6,5 Terabytes en un objetivo. • Objetivos → Países de habla inglesa • Detectado: 2006. MANDIANT
NetTraveler:	• Junio 2013. • Actividad desde 2005 [2010-2013]. • 350 víctimas – 40 países, incluyendo gobiernos, investigación, activistas y periodistas. • Más de 22 GB de datos robados. Espionaje básico, distintos *backdoors*. • Detectado: KASPERSKY
Icefog:	• Activo desde 2011. • Países objetivo: Principalmente de Japón, Corea del Sur y Taiwán. • Víctimas → sector gubernamental, contratistas de Defensa, grupos de construcción e infraestructuras, operadores de telecomunicaciones, compañías de alta tecnología y medios de comunicación. • Vectores de ataque: spear-phishing (mediante exploits de Microsoft Office, Java exploits, vectores HLP y vectores HWP). • Detectado: KASPERSKY

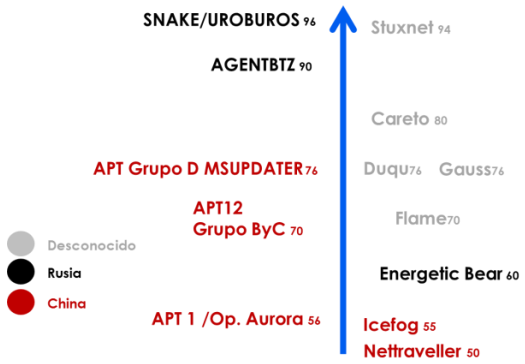
Obviamente, no todas las APTS poseen el mismo grado de sofisticación. Se realiza una clasificación de los mismos de 1 a 100 según los siguientes criterios:

- **Características técnicas (valoración máxima de 60)** donde se valora la capacidad de desarrollo, especialmente de las vulnerabilidades utilizadas (día cero, fecha de publicación…), las herramientas utilizadas (propietarias o no), el cifrado (fortaleza e implementación), las técnicas de ex filtración (uso de protocolos estándar / propietarios), las técnicas de persistencia, su ocultación en el sistema (capacidades de evitar la detección por antivirus u otras herramientas de seguridad).

- **Características de operación (valoración máxima de 40)** donde se valora la interacción del atacante sobre sistema infectado, su grado de conocimiento del

mismo y los procedimientos empleados por su personal. Se valora además las técnicas de Ingeniería social para realizar las infecciones, los procedimientos para seleccionar objetivos y las características técnicas de su infraestructura (ocultamiento del direccionamiento IP origen del ataque, número de saltos, servidores de mando y control,…)

La figura siguiente muestra el esquema de complejidad de las APTs más significativas[37].



Durante 2013, España no ha sido ajena a este tipo de ataques dirigidos, que han puesto el foco, especialmente, en las empresas tecnológicas (en muchas ocasiones, contratistas del sector público) y en los propios organismos de las AAPP (Administración General del Estado, de las Comunidades Autónomas y agencias y entidades dependientes, así como algún ayuntamiento importante).

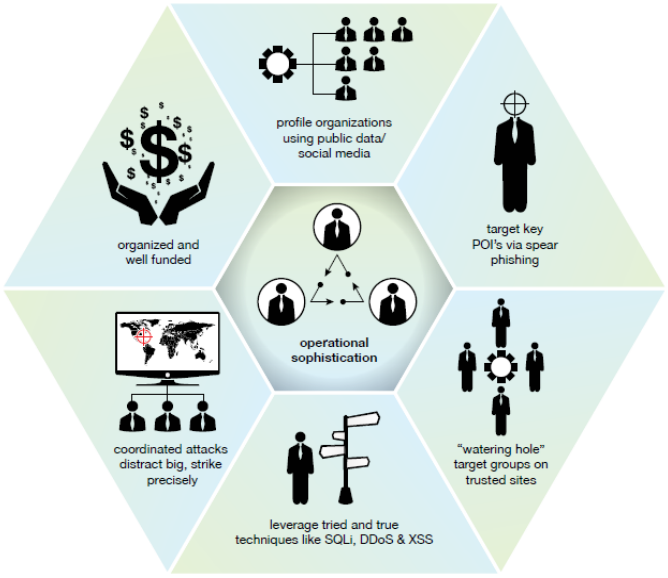
Las APTs contra organizaciones y contra personas

2013 se inició con una serie de ataques muy sofisticados (operativa y técnicamente) y de perfil alto contra diferentes entidades: reputados sitios web, medios de comunicación, empresas de alta tecnología y organismos públicos.

La **sofisticación operativa** consistió, básicamente, en que los atacantes utilizaron rutas selectivas que les permitieron obtener la máxima rentabilidad de los exploits. Para ello, usaron un amplio conjunto de técnicas muy probadas, tales como la inyección SQL (SQLi), el Cross Site Scripting (XSS) y la suplantación de identidad, así como la explotación de aquellas plataformas software que poseen un mayor parque de usuarios, tales como Adobe Flash y los plug-in Java de los navegadores. Por otro lado, el atacante, al objeto de conocer todo lo posible el comportamiento de su víctima, empleó la información disponible en las redes sociales y de otros documentos que hubieran sido indexados por los motores de búsqueda. La figura siguiente muestra un diagrama de la sofisticación de los métodos de ataque usados[38].

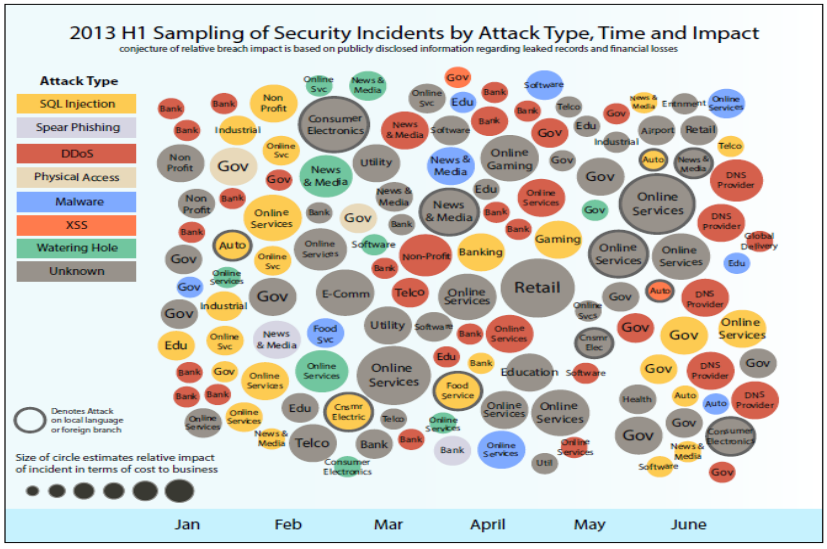
37 Alguna de las APTs referenciadas en el esquema han aparecido ya en 2014.

38 IBM X-Force 2013 Trend and Risk Report



La sofisticación de los métodos de ataque usados

En el otro lado, la **sofisticación técnica** se basa en el uso de ataques avanzados tales como la explotación de vulnerabilidades de día-cero. La figura siguiente muestra un mapa de los incidentes de seguridad ocurridos durante el primer semestre de 2013, por tipo de ataque, tiempo e impacto.



Ejemplos de incidentes de seguridad durante el primer semestre de 2013, por tipo de ataque, tiempo e impacto

Por otro lado, estas amenazas, en 2013 han utilizado a altos directivos de compañías y de organismos públicos, personajes notorios y responsables políticos como medio de acceso a empresas e instituciones públicas. Es de destacar que una vez que los atacantes han conseguido del ordenador de la víctima la información perseguida, suelen eliminar sistemáticamente las pruebas de su ataque, borrando el código dañino instalado en estos dificultando la investigación. Las víctimas son reticentes a denunciar estos ataques.

Tratándose de ataques tipo APT, uno de los problemas más importantes es considerar el tiempo que tarda en ser remediada la situación. En principio se estima en meses lo que se emplea un ataque de este tipo. El cuadro siguiente resume algunas noticias de prensa con la valoración del impacto recibido.

Departamento de Defensa de EE.UU.: El 27 de mayo de 2013, el *Washington Post* informó que hackers chinos habían penetrado en los sistemas de información del Departamento de Defensa y habían sustraído los diseños de varias armas (sistemas de defensa de misiles balísticos anti-misiles). También se sustrajeron diseños de aeronaves y buques. A principios de año, el Defense Science Board, compuesto por expertos del gobierno y del sector privado y del mundo académico, concluyó que los EE.UU. no están preparados para una ciberguerra a gran escala.	**Gobierno de Pakistán:** El 21 de mayo de 2013, el *Information Week* informó de un ataque lanzado contra el gobierno de Pakistán y organizaciones relacionadas con explotaciones mineras, empresas automovilísticas, militares y de ingeniería. Se sospecha de un posible origen en India, habiendo comenzado en 2010 (o quizás, antes). Este ataque utilizó más de 600 dominios y 800 piezas de código dañino, algunos de las cuales fueron adaptadas a objetivo.
New York Times: En enero de 2013, el *New York Times* publicó un informe que afirmaba que hackers chinos, se habían infiltrado en sus redes. El ataque parecía ser consecuencia de una investigación del periódico que reveló que los familiares del entonces primer ministro chino habían acumulado una gran fortuna en diferentes negocios. Se cree que el ataque fue iniciado mediante una campaña de spear-phishing, Los ataques fueron diseñados para buscar mensajes de correo electrónico saliente y documentos relacionados con la historia publicada por el New York Times, para descubrir las fuentes de la noticia. El New York Times declaró que los ataques no habían tenido éxitos. Tras esta noticia, Bloomberg LP, Wall Street Journal y Washington Post informaron de que también habían sido objetivos de ataques, posiblemente chinos.	

Las herramientas comerciales de acceso remoto ganan popularidad entre los agentes del ciberespionaje

Tradicionalmente, este tipo de atacante venía construyendo su propio código dañino para introducirse en las redes infectadas[39] y, desde allí, exfiltrar datos al exterior. Tales herramientas ad hoc, aunque muy difíciles de detectar por los antivirus comerciales, han sido, sin embargo, objeto de un mayor estudio en los últimos años, lo que ha permitido identificar grupos específicos basándose en los atributos de este software particularizado.

En 2013, sin embargo, se ha apreciado un significativo aumento en el número de ataques realizados con herramientas RAT[40] comerciales –código abierto o de libre acceso-, que se utilizan para controlar los sistemas comprometidos. El motivo de esta nueva tendencia habrá que situarlo en dificultar la atribución de un ataque, aunque se proporcione a las organizaciones atacadas mayores posibilidades de detección sobre estos RAT que si se tratara de herramientas personalizadas.

39 Este código dañino que penetra en las redes de las víctimas suele denominársele payload.

40 RAT – Remote Access Tool.

Algunas herramientas RAT como Poison Ivy son muy utilizadas en campañas de ciberespionaje, aunque también se ha advertido el uso de otras RAT "comerciales" y variantes modificadas de código abierto, tales como Gh0stRAT. La compañía Verisign, ha podido comprobar la presencia de **código común en Gh0stRAT, Lurk, Melody, PCRat y NetShark**, siendo todas ellas empleadas en ataques detectados en 2013.

En cuanto a las RAT más recientes, se ha podido observar el uso de FrustasRAT[41], y BozokRAT (ataque contra el Banque de France[42]). La utilización de estas nuevas herramientas RAT, demuestra la búsqueda de nuevas RAT de código abierto para añadir a sus herramientas de ataque. Es presumible que, en 2014, se aprovechen técnicas utilizadas en el desarrollo de código dañino propio con el fin de modificar las RAT de código abierto, para eludir la capacidad de detección de las herramientas de seguridad y los antivirus. Un ejemplo es el uso de un troyano para cifrar las RAT comerciales. En 2013, se detectaron muestras de DoWork[43], que se entregaba como payload de documentos dañinos creados por la herramienta MNKit.

Otra táctica utilizada contempla el uso de ejecutables legítimos -firmados mediante certificados válidos- que cargan una biblioteca DLL dañina, así, el atacante carga su DLL dañina dándole el mismo nombre que el de una biblioteca legítima. Por ejemplo, se han utilizado ejecutables firmados como RasTls.exe (Symantec's Network Access Control) y Gadget.exe (Tencent's SideBar), entre otros, para ejecutar archivos DLL dañinos denominados RasTls.dll y SideBar.dll, respectivamente. Estas DLL dañinas descifran y ejecutan un tercer archivo que contiene el código del troyano DestroyRAT (PlugX).

Estos ataques usando las RAT "comerciales" se han detectado en un amplio abanico de objetivos, por lo que muchas organizaciones podrían estar expuestas a este tipo de ataque que, se espera se incremente en 2014.

El uso de RCS por los gobiernos

En 2013, se ha alertado del uso por muchos gobiernos del llamado RCS (Remote Control System), un software muy sofisticado, creado por la empresa italiana Hacking Team[44], y que se vende exclusivamente a gobiernos. La figura siguiente muestra una estimación del empleo detectado de este software a finales de 2013.

41 iDefense Security Intelligence Services. "Cyber Espionage Threat Actors Leverage FrutasRAT against Japanese and Russian Government Ministries" (ID# 952114, v.3, Sept. 19, 2013).

42 iDefense Security Intelligence Services. "Targeted Attack on Banque de France Uses WingD to Install BozokRAT" (ID# 973564, v.3, Nov. 1, 2013).

43 Falcone, Robert. "DoWork: Connecting Various Tools to SILVERVIPER." Oct 10, 2013. iDefense Security Intelligence Services. https://idefense.verisign.com/group/idefense/search?_irSearch_blogEntryId=b6efafaa-b267-4ac7-8c34-9531a83e18fb&_irSearch_blogType=14

44 http://hackingteam.it/index.php/customer-policy

21 SUSPECTED GOVERNMENT USERS

AMERICAS	EUROPE	MIDDLE EAST	AFRICA	ASIA
Mexico	Hungary	Oman	Egypt	Azerbaijan
Colombia	Italy	Saudi Arabia	Ethiopia	Kazakhstan
Panama	Poland	UAE	Morocco	Malaysia
	Turkey		Nigeria	Thailand
			Sudan	South Korea
				Uzbekistan

6.3.2 La ciberdelincuencia

Ataques contra Terminales Punto de Venta y Cajeros Automáticos

Durante 2013 se observó un marcado aumento de código dañino dirigido a Terminales Punto de Venta (TPV) y, en menor medida, a Cajeros Automáticos.

Los mecanismos de ataque aprovechan que tales dispositivos suelen estar conectados a Internet para facilitar su administración, y lo que, al mismo tiempo, favorece la penetración de código dañino. Normalmente se emplean contraseñas débiles que permiten a los atacantes explotar las tecnologías Remote Desktop Protocol (RDP) y Virtual Network Computing (VNC), que posibilitan la adquisición remota de datos de tarjetas de crédito o débito.

Entre el código dañino para TPV aparecido en el mercado negro en 2013, figuró el siguiente[45]:

- ***Alina***[46] (precio: $5.000; detectado en octubre de 2012).
- ***BlackPOS***[47] (precio: $1.800-$2.300; detectado en febrero de 2013).
- ***Dexter***[48] (precio: $3.000; detectado en diciembre de 2012)
- ***Project Hook***[49] (precio: 10 Bitcoins [aproximadamente $6.000 a 20 de diciembre 2013]; detectado en mayo de 2013).
- ***vSkimmer***[50] (precio: $5.000 - $6.000; detectado en diciembre de 2012).

45 iDefense: 2014 Trends.

46Davenjah. "POS Código dañino – Alina v6.0 & Dexter v2 StarDust." inFraud – Faculty Researching of Dead Presidents. https://infraud.cc/showthread.php?t=16816

47 Ree[4]. "Dump CC Memory Grabber (POS Trojan)." April 12, 2013. Exploit.in. https://exploit.in/forum/index.php?showtopic=66616&view=findpost&p=415567

48Davenjah. "POS Código dañino – Alina v6.0 & Dexter v2 StarDust." inFraud – Faculty Researching of Dead Presidents. https://infraud.cc/showthread.php?t=16816

49 Op. cit.

Además se está empleando software que posea capacidades de administración remota. Un ejemplo de este tipo de código dañino es RDPxTerm, que crea conexiones RDP, siendo capaz de recopilar información acerca de los sistemas de pago de la máquina infectada[51].

En relación con los Cajeros Automáticos, en 2013 se descubrieron dos puertas traseras: Ploutus y Trojan[52]. Ploutus era un troyano dirigido inicialmente contra cajeros automáticos de América Latina, especialmente de México, y que ha venido evolucionando desde entonces para atacar los cajeros automáticos en otros países de habla inglesa. A diferencia del código dañino para TPV, Ploutus no captura datos de la tarjeta, sino que su objetivo es dispensar dinero en efectivo. La infección de un cajero automático se produce mediante acceso físico al mismo insertando un disco de arranque en la unidad de CD- ROM. En este caso, sólo es capaz de dispensar dinero en efectivo de un cajero automático infectado dentro de las 24 horas siguientes a la activación del código dañino.

En diciembre de 2013, el proveedor de antivirus con sede en Rusia Dr.WEB descubrió un backdoor llamado **Trojan.Skimmer**, construido para acceder a los datos de la banda magnética. Este código dañino permitía el acceso al PIN.

El 18 de diciembre de 2013, se informó de un ataque que afectó a la entidad norteamericana Target Corporation[53]. Entre el 27 de noviembre y 15 de diciembre, se comprometieron los datos de las tarjetas bancarias de más de 110 millones de compradores[54]. En este caso, el vector de ataque fue un código dañino muy similar a BlackPOS.

Por su parte, la rápida evolución del código dañino para dispositivos TPV podría sugerir una tónica similar para los cajeros automáticos en 2014. Aunque tienen la limitación del acceso físico.

La actividad legítima e ilegitima de Bitcoin

En mayo de 2013, el gobierno de EE.UU. clausuró la moneda electrónica elegida por muchos ciberdelincuentes: Liberty Reserve. Por ello, muchos ciberdelincuentes han venido buscando una nueva moneda electrónica inmune a tales clausuras. Bitcoin ha ganado fuerza en este sentido, a pesar de su más que inestable tasa de cambio. Por otro lado, esta moneda virtual ha comenzado a ganar aceptación en actividades legítimas, con la creación de entidades como BitPay[55], Coinbase[56] y SnapCard[57], por lo que resulta cada vez más fácil a las

50 Beast. "vSkimmer – Track 2 Grabber/POS Trojan." December 6, 2012. Omerta – The World is Yours. http://omerta.cc/showthread.php?t=14403

51ReV. "RDPxTerm 5.1 (Build 4.4.2) Private Edition, Modification RDPxTerm." March 27, 2013. Exploit.in. https://exploit.in/forum/index.php?showtopic=67556

52Regalado, Daniel. "Backdoor.Ploutus Reloaded – Ploutus Leaves Mexico." Oct. 25, 2013. Symantec. http://www.symantec.com/connect/blogs/backdoorploutus-reloaded-ploutus-leaves-mexico

53 Target Corporation es una cadena de grandes almacenes, fundada en Minneapolis, Estados Unidos, en 1962.

54 Harris, Elizabeth H. and Nicole Perlroth. "For Target, the Breach Numbers Grow." Jan. 10, 2014. The New York Times. http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html

55 https://bitpay.com/

56 https://coinbase.com/

empresas aceptar Bitcoins en sus transacciones. Así, un número creciente de compañías están empezando a aceptar o considerando aceptar Bitcoins, incluyendo entre ellas a Overstock.com[58], TigerDirect[59], Google Inc.[60] y eBay[61].

Este tipo de moneda supone un reto regulatorio para los gobiernos e instituciones, que pretenden prevenir comportamientos delincuenciales. Históricamente, las autoridades han estado por detrás de los acontecimientos cuando se trata de monedas electrónicas. Por ejemplo, cuando las autoridades rusas intentaron actuar sobre la moneda electrónica WebMoney, ya fue demasiado tarde. Esta moneda, que es usada por muchos ciberdelincuentes, ha sido aceptada por otros clientes legítimos, que no quieren utilizar opciones de banca tradicional. La situación actual es de compromiso: las autoridades permiten a WebMoney operar a nivel internacional y, a cambio, WebMoney coopera con las autoridades para investigar casos criminales importantes.

No sucedió lo mismo con Liberty Reserve. Cuando el Departamento de Justicia de EE.UU. tomó medidas, no existía un bloque de empresas legítimas que se opusiera a su clausura. Además, esta moneda no tenía tanta importancia en la economía de los EE.UU. como lo tenía WebMoney en Rusia.

Una prohibición total de Bitcoin (dada su popularidad y su descentralización) sería difícil y de dudosa legalidad. Esta moneda no posee una organización central y una regulación global que le sea de aplicación. No obstante en EE.UU, el Internal Revenue Service (IRS)[62] abrió expediente a 24 elementos de intercambio de Bitcoin. Por otra parte, la Government Accounting Office (GAO) publicó un informe sobre los riesgos de Bitcoin relacionados con el blanqueo de dinero y la exención fiscal. Por su parte, la US Treasury's Financial Crimes Enforcement Network (FinCEN) desarrolló normas respecto a Bitcoin. El IRS ha anunciado planes para hacer lo mismo.

Toda esta actividad condujo a que algunos intercambios Bitcoin no pudieran llevarse a cabo. Así, algunos funcionarios norteamericanos congelaron las cuentas en EE.UU. del servicio de intercambio de Bitcoin con sede en Tokio: Mt. Gox, mientras que el US Department of Homeland Security prohibió el servicio de pagos en línea Dwolla, en relación con el intercambio de, aproximadamente, 5 millones de dólares en Bitcoins, en poder de Mt. Gox.

China también está intentando regular esta situación. En mayo de 2013, China superó a todos los demás países con 84.000 descargas de Bitcoins, y, en octubre, BTC China superó a Mt. Gox como el mayor intercambiador de Bitcoin del mundo. Esta popularidad se debe a la

57 https://www.joinsnapcard.com/

58Phillips Erb, Karen. "Will Overstock Force IRS To Make Up Its Mind About Bitcoin?" Jan. 13, 2014. Forbes. http://www.forbes.com/sites/kellyphillipserb/2014/01/13/will-overstock-force-irs-to-make-up-its-mind-about-bitcoin/

59 TigerDirect.comNow Accepts Bitcoin Payments!" Accessed on Jan. 23, 2014. TigerDirect.com. http://www.tigerdirect.com/bitcoin/

60Rizzo, Pete. "Leaked Emails From Google Suggest it is Considering Bitcoin Integration." Jan. 23, 2014. Coin Desk. http://www.coindesk.com/google-emails-suggest-bitcoin-interest/

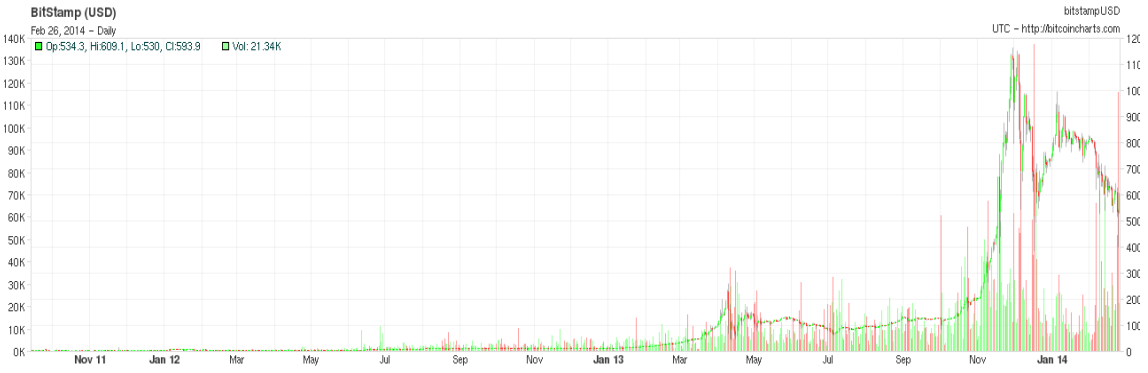
61 Berniker, Mark. "EBay considering accepting bitcoin as payment." Jan. 23, 2014. CNBC. http://www.cnbc.com/id/101356642

62 El IRS (Internal Revenue Service) es la agencia norteamericana responsable de la recolección de impuestos y la persecución de los delitos fiscales.

atracción que despierta Bitcoin entre los especuladores, debido en parte a la escasez de alternativas para los pequeños inversores en China[63]. El 5 de diciembre de 2013, las autoridades chinas prohíben a las instituciones financieras la negociación de Bitcoins. La mayor empresa china de servicios web Baidu acató la sentencia, rechazando el pago en Bitcoins.

Además de las iniciativas regulatorias de EE.UU. y China, otros países parecen estar tomando decisiones similares. Por ejemplo, Singapur, Alemania y el Reino Unido sostienen el criterio de que Bitcoin es una moneda y que las transacciones en tal moneda deben estar sujetas a impuestos[64]. En contraposición, la India contempla Bitcoin como un producto de inversión en peligro de sobrecalentamiento. Así, The Indian Reserve Bank hizo público un aviso en el que detallaban los riesgos de Bitcoin, al tiempo que las firmas de intercambio se enfrentaban a acciones legales por violar las regulaciones monetarias[65].

Por otro lado, la estabilidad de Bitcoin está lejos de resolverse totalmente. Por ejemplo, en el caso de China, el anuncio de las restricciones financieras, junto con los comentarios negativos respecto a las perspectivas de Bitcoin hechos por el Banco de Francia y el ex presidente de la Reserva Federal, Alan Greenspan, hizo que el precio de un Bitcoin cayera desde 1.200 dólares a 900 dólares a principios de diciembre de 2013. Además, la noticia de que BTC China –y otros- no podían aceptar la moneda redujo el valor del Bitcoin a menos de 400 dólares[66]. En la figura adjunta se muestra el cambio de esta moneda durante 2013.



Para evitar la aplicación de las regulaciones existentes, se están ofertando servicios que permiten a los usuarios a evitar ser detectados eliminando la necesidad de utilizar un cambio

63Hu, Jack. "Chinese Web Giants Alibaba, Baidu Launch Online Investment Funds for the Everyman." Dec. 11, 2013. Global Voices. http://globalvoicesonline.org/2013/12/11/chinese-web-giants-alibaba-baidu-launch-online-investment-funds-for-the-everyman/

64Phillips Erb, Kelly. "UK Bows To Pressure, Likely To Reverse Course On Taxation Of Bitcoin: Will The US Be Next?" Jan. 17, 2014. Forbes. http://www.forbes.com/sites/kellyphillipserb/2014/01/17/uk-bows-to-pressure-likely-to-reverse-course-on-taxation-of-bitcoin-will-the-us-be-next/

65Metz, Cade. "Bitcoin Exchanges Shut Down in India After Government Warning." Dec. 27, 2013. Wired. http://www.wired.com/business/2013/12/bitcoin-india/

66 Gough, Neil. "Bitcoin Value Sinks After Chinese Exchange Move." Dec. 18, 2013. The New York Times. http://www.nytimes.com/2013/12/19/business/international/china-bitcoin-exchange-ends-renminbi-deposits.html?hp&_r=1&gwh=DEC4A2D210F9BCAEB74B045DFF1609EE&gwt=pay&

conocido, mediante el uso de e tarjetas anónimas, o de tarjetas nominativas no totalmente verificadas por los emisores, algunos de cuyos ejemplos se muestran en la figura siguiente.

A medida que Bitcoin aumente en popularidad, será más fácil para los ciberdelincuentes ocultar sus transacciones o ganancias ilícitas, lo que incrementará el uso de Bitcoins por estos, ya sea en el momento de pagar servicios delictivos, en la aceptación de rescates obligados por el ransomware o en el blanqueo de dinero.

Sin embargo, como decimos, los atacantes no son los únicos usuarios de Bitcoin. Los usuarios "legales" posibilitan a los organismos reguladores la oportunidad de reorientar la moneda hacia un escenario transparente. Los EE.UU., China y cualquier otro país cuyos ciudadanos utilicen Bitcoins tendrán que encontrar un medio coherente de incorporar controles legales para observar y prevenir actividades ilegales. Las instituciones, especialmente las financieras y comerciales, deben también determinar políticas para encarar el fenómeno Bitcoin, tarea nada fácil para algo que es visto, alternativamente, como una mercancía, una moneda, una herramienta delictiva y hasta una posible alternativa a los actuales sistemas nacionales. 2014 será un año importante para Bitcoin, en el que, presumiblemente, podrá definirse la dirección futura de esta moneda[67].

Las herramientas de los ciberdelincuentes: Los exploits-kits

Como hemos señalado en nuestros Informes de Amenazas de los pasados años, desde 2011, muchos grupos de ciberdelincuentes han sustentado sus acciones en base a la utilización de exploits-kits -como Blackhole[68] y otros- para obtener provecho de las vulnerabilidades de los sistemas e instalar código dañino. Así, por razón de su precio, su facilidad de uso, el soporte técnico y la eficiencia, Blackhole ha sido el exploit kit más usado desde 2011.

En abril de 2013, las autoridades rusas detuvieron al presunto autor de un exploit-kit muy conocido: Phoenix[69]. Unos meses más tarde, el 8 de octubre de 2013, Reuters informó que las autoridades rusas habían arrestado a un individuo de nombre –Paunch-, autor y vendedor de dos exploit-kit igualmente populares: Blackhole y Cool[70].

Como la noticia de la detención de Paunch se extendió rápidamente por la comunidad de seguridad y los foros clandestinos, los grupos de ciberdelincuentes modificaron sus hábitos de distribución de código dañino, suspendiendo el soporte a los exploits-kits ya vendidos.

67 Al tiempo del cierre de esta edición, Mt.Gox ha clausurado (¿temporalmente?) su actividad.

68 iDefense Security Intelligence Services. "State of the Blackhole Exploit Kit in 2013." (ID# 949673, Dec. 17, 2013).

69 Krebs, Brian. "Phoenix Exploit Kit Author Arrested in Russia?" April 8, 2013. Krebs on Security. http://krebsonsecurity.com/2013/04/phoenix-exploit-kit-author-arrested-in-russia/

70 Finkle, J. and J. Menn. "Suspect in 'Blackhole' cybercrime case arrested in Russia." Oct. 8, 2013. Reuters. http://www.reuters.com/article/2013/10/08/cybercrime-arrest-idUSL1N0HY26I20131008

La figura siguiente muestra los exploits-kits que, actualmente, están siendo usados para reemplazar a Blackhole[71].

Criminal Group Alias	Malware Distributed	Exploit Used to Distribute Malware	Exploit Used After Paunch's Arrest
Mr.J MonsterAV	Reveton Ransomware, Fake AV	Cool	Whilehole, Angler
Home Gang	Pony, ZeroAccess	Darkleech	Blackhat SEO
Ex-Trk	Carberp	Blackhole	Neutrino
/topic/	Pony, ZeroAccess, Opus, FakeAV	Blackhole	Upatre Downloader
/ngen/	Citadel, Shylock, ZeroAccess	Blackhole	Blackhole
/news/	Opus, Blockade	Blackhole	Magnitude (Popads)
/vague/	Citadel	Blackhole	Nuclear Pack

Del cuadro anterior se desprende que los ciberdelincuentes no han encontrado todavía un único sustituto de Blackhole. De hecho, algunos actores han recurrido a métodos más simples de distribución de código dañino, incluyendo descargas drive-by o, simplemente, agregando código dañino a los e-mails y usando ingeniería social.

A partir del cuarto trimestre de 2013 se han evidenciado dos hechos:

1. los exploits-kits Neutrino, Angler, Kein y Styx tratan de ocupar el espacio dejado por Blackhole

2. se ha apreciado un aumento de los correos electrónicos de phishing que adjuntan código dañino, tales como los descargadores Upatre y Pony y los troyanos bancarios Opus, Blockade y Hesperus.

Es razonable suponer que en 2014 los exploits-kits más eficaces agruparán a la mayor parte de los antiguos clientes de Blackhole. Neutrino, Angler y Nuclear Pack constituyen buenos candidatos que ya están aumentando su base de usuarios. El fin de Blackhole no significa que los ciberdelincuentes hayan dejado de usar exploits-kits.

6.3.3 El Hacktivismo

Anonymous y la "balcanización" del hacktivismo

Durante los últimos años se ha observado una importante tendencia a la regionalización de los grupos hacktivistas. Anonymous, el grupo hacktivista más publicitado de los últimos años, se ha dividido en varios grupos. Así, han aparecido una amplia gama de grupos hacktivistas más pequeños, a veces etiquetados como subconjuntos regionales de Anonymous, y que están jugando un papel cada vez más importante en estos ataques.

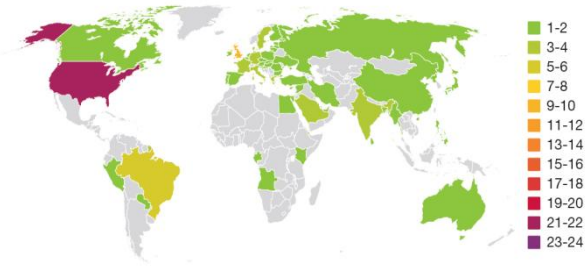
En cierto modo, esta tendencia puede marcar un regreso al paisaje hacktivista de los días pre-Anonymous. A pesar de que Anonymous ha sido objeto desde sus orígenes de importantes y continuas investigaciones, el hacktivismo tuvo su origen en pequeños grupos de hackers,

71 Fuente: Kafeine. "Paunch's arrest... The end of an Era !" Accessed on Dec. 16, 2013. Código dañino don't need Coffee. http://código dañino.dontneedcoffee.com/2013/10/paunch-arrestationthe-end-of-era.html

cuyas acciones se concentraban esencialmente en asuntos regionales o nacionales, tales como los grupos que participaron en la guerra de hackers chino-indonesia de 1998[72]. No obstante, el relativo éxito del Proyecto Chanology de 4chan, la posterior crisis financiera de 2008 y la saga de WikiLeaks popularizó la ideología y el modus operandi de Anonymous.

Actualmente, como decimos, los hacktivistas están formando, cada vez más, sus propios grupos de acción local o, incluso, de disidentes de Anonymous (tales como Anonymous Brasil, Australia, Corea, etc.) De esta manera, el concepto del movimiento Anonymous como "colectivo" se está fracturando en beneficio de acciones regionales o nacionales.

La figura siguiente muestra el disperso mapa de objetivos durante 2013.



En la figura se observa que, aunque un importante número de operaciones hacktivistas continúan atacando a entidades del mundo occidental (fundamentalmente, de los EE.UU. y Europa del Este), el impacto de las campañas hacktivistas contra los gobiernos y los empresarios de otras regiones está en franco crecimiento.

En 2013, las denuncias de corrupción de los gobiernos, las manifestaciones por la degradación ambiental y las protestas por los altos costes de la electrónica importada estimularon la actividad hacktivista en Brasil[73]. Del mismo modo, la desilusión con las industrias del petróleo y las entidades financieras, y las supuestas prácticas laborales explotadoras condujo a los ciberataques contra gobiernos y empresas en Arabia Saudí74 y los Emiratos Árabes Unidos75, mientras que la indignación por la revelación de la complicidad de Australia en el espionaje de la National Security Agency (NSA) contra diplomáticos de Indonesia provocó un enfrentamiento entre los hacktivistas de Indonesia y Australia76.

Es de esperar un incremento del hacktivismo (global o regional) como forma legítima (o no) y efectiva de protesta social.

72 "Chinese protesters attack Indonesia through net." Aug. 19, 1998. BBC.
http://news.bbc.co.uk/2/hi/science/nature/154079.stm

73 iDefense Security Intelligence Services. "OpBoicoteaCopa/OpBoycottCup."

74 iDefense Security Intelligence Services. "OpSaudi."

75 iDefense Security Intelligence Services. "OpDubai/OpUAE."

76 iDefense Security Intelligence Services. "OpAustralia.".

El hacktivismo en Iberoamérica

Durante 2013, podemos distinguir dos fases temporales respecto del escenario hacktivista en Iberoamérica, así como dos áreas geográficas diferenciadas en cuanto a la expresión del fenómeno. En el primer semestre se detecta una actividad sostenida en México y Brasil y, en menor medida, en Chile y Argentina; para posteriormente decaer la actividad en México, Chile y Argentina en el segundo semestre y mantenerse en Brasil.

En cuanto a áreas geográficas diferenciadas, tanto por actividad cualitativa como cuantitativa, la expresión del hacktivismo en Brasil ha venido siendo distintiva del resto del subcontinente, con Brasil integrando muy marcadamente la cibermilitancia y el activismo sobre el terreno físico a través no solo de Anonymous sino de células con orientación anarquista de acción directa como Black Bloc o los Ninjas.

En el primer semestre de 2013, las instituciones de gobierno nacionales y federales de México y Brasil han sido blanco preferente de ciberataques. Además de este patrón sudamericano, ha sido apreciable un incremento de actividad en Centroamérica, cubriéndose prácticamente todos los países del istmo menos Nicaragua y Belice en ataques y con operaciones definidas en Costa Rica, Honduras, Guatemala y El Salvador. Así mismo han sido relevantes marcos de ciberataque contra medios de comunicación en Brasil, en línea con el abandono ya internacional de la restricción de ataque a medios de comunicación que se había marcado Anonymous.

En las operaciones hacktivistas del primer semestre de 2013 en Iberoamérica, los ciberespacios de México y Brasil han sido objeto de operaciones específicas de Anonymous en apoyo de manifestaciones de colectivos tipo 15M u occupy sobre el terreno. También ha sido observable durante 2013 operaciones que, iniciadas en un país, dan el salto a otro, facilitadas por la colaboración transnacional inter-grupos entre facciones Anonymous en el marco del conglomerado conocido como Anonymous Iberoamérica.

Anonymous Iberoamérica es una conjunción de grupos afiliados a Anonymous en varios países de América Latina coordinada (presuntamente) por un nacional colombiano. El conglomerado Anonymous Iberoamérica, tras una disensión interna con componentes de Anonymous Chile, se ha convertido en clúster generador de facciones nacionales de Anonymous en el subcontinente, además de un proveedor continuo de ciberoperaciones en varios de los ciberespacios sudamericanos.

En el último tercio de 2013 en Iberoamérica, cabe destacar igualmente el descenso de actividad de Anonymous en México y Chile (que se supone coyuntural); y la acción de la facción LulzSecPerú contra sistemas del Ministerio del interior del Perú, que ha supuesto la exfiltración de documentación clasificada y de operaciones de la Policía Nacional del país.

En lo que respecta a Brasil, se subraya la fuerte implantación de colectivos Anonymous en la organización de manifestaciones antigubernamentales desarrolladas sobre el terreno en el plano físico, además de la activación ciberataques, en varias ciudades del país, en coalición con agrupaciones anarquistas de Black Bloc, agrupaciones que están a favor de aplicar la violencia contra símbolos del "capital". A finales de 2013 se iniciaron ataques y convocatorias, igualmente con correlación entre ciberataques de Anonymous y protestas de grupos anarquistas en el plano físico, en el marco de la #OpWorldCup u #OpBoicoteaCopa contra la copa mundial de fútbol de 2014 y bajo la consigna de "Nao Vai Ter Copa". Estos ciberataques

en el marco de #OpBoicoteaCopa, que se han venido produciendo preferentemente contra webs de gobierno en Brasil, se han articulado principalmente por células de reciente creación; compuestas por entre dos y tres identidades; afiliadas a Anonymous Brasil pero adoptando cada una de ellas su propia denominación; y con capacidades técnicas, al menos, para producir defaces aprovechando vulnerabilidades web. En ese contexto operativo, en hacktivismo con procedimientos Anonymous en Brasil se ha venido expresando a finales de 2013 y principios de 2014 a través de denominaciones como InsanityHackteam, DKBrazilHackTeam, Invaders of Security o Black Devil's.

El hacktivismo internacional

En el plano internacional, la actividad ofensiva hacktivista ha descrito tres direcciones: operaciones tradicionales tipo Anonymous reaccionando contra mecanismos de control en Internet o promoviendo filtraciones de información; marcos de ciberataque contra los ciberespacios de varios países, preferentemente EE.UU. e Israel, ejecutados por ciberidentidades con iconografía árabes y apoyados en narrativas combinando elementos políticos (revueltas árabes) o nacionalistas (p.ej. defensa de Palestina) con islamistas; y desarrollos como la #OpGreenRights, que involucra una narrativa militante sobre una causa específica (la medioambiental) para programar fases de ciberataque contra webs de empresas o gobiernos involucrados en proyectos vinculados a esa narrativa militante.

En la primera dimensión de las **narrativas contra legislaciones de control en Internet**, 2013 ha visto operaciones, generalmente de baja intensidad, como las #OpBBC, #OpBigBrother u #OpPrism/#OpNSA, dirigidas contra webs de gobierno o empresas de telecomunicaciones y organizadas por ciberidentidades anglosajonas. Estas propuestas hacktivistas, aunque planteadas casi siempre con fuerte aparato propagandístico (narrativas motivadas en textos alojados en plataformas 'paste', vídeos, iconos diseñados para redes sociales), no han tenido poder de convocatoria suficiente como para producir efectos apreciables durante 2013, tal vez por la ausencia de un liderazgo claro unificador en el plano internacional.

En la segunda de las dimensiones, las iniciativas generalmente desde conglomerados de identidades con iconografía árabe contra ciberespacios de varios países, han destacado denominaciones como #OpEgypt, #OpIsrael, #OpSyria, #OpTurkey u #OpUSA. Todas ellas han sido propuestas de ciberataques masivos, concentradas en pocos días, llevadas a cabo contra cientos webs de bajo perfil principalmente con acciones por deface combinados con inyecciones SQL, y ejecutadas por coaliciones de ciberidentidades árabes, casi todas ellas organizadas o participadas por el grupo AnonGhost.

En el mismo plano de operaciones organizadas por conglomerados de identidades árabes se han lanzando en 2013 iniciativas no tanto contra ciberespacios nacionales como basadas en narrativas específicas, como #OpPetrol, promovida por AnonGhost contra determinadas empresas y naciones petroleras; u #OpAbabil, organizada por el grupo Izz ad-Din al-Qassam Cyber Fighters y ejecutada en varias fases durante 2013 contra webs de entidades financieras en EE.UU.

Dentro del escenario militante de revueltas en países árabes, en torno a Siria se ha mostrado muy activa durante 2013, como hemos señalado en epígrafes anteriores, la ciberidentidad Syrian Electronic Army (SEA), presumiblemente apoyada desde el gobierno sirio y que ha venido atacando, principal aunque no únicamente, webs y perfiles en redes sociales

de medios de comunicación estadounidenses y británicos, aplicando para ello técnicas más sofisticadas que las habituales inyecciones XSS y SQL: el SEA ha combinado tácticas de phishing con el uso de exploits y bots para lanzar sus ataques.

Por último, ha destacado internacionalmente durante 2013 la #OpGreenRights que, organizada y ejecutada desde Anonymous en Italia con una narrativa medioambientalista, ha sido muy activa tanto en procedimientos de exfiltración como en la ejecución de ataques DDoS, principalmente contra empresas y contra webs de gobierno en distintos países.

En términos de logística hacktivista en el ámbito internacional, cabe subrayar el mayor uso de la plataforma cyberguerrilla.org como núcleo de reunión y organización de facciones Anonymous, que durante 2013 han migrado sus canales de IRChat desde otras plataformas (como anonops.com). Desde cyberguerrilla.org también se están postulando nuevos sistemas de comunicación para Anonymous a través de TOR, ideas de momento en fase de planeamiento.

El hacktivismo en manos de los Estados

2013 fue testigo del aumento de las operaciones de estética hacktivista en el contexto de actividades dirigidas por los Estados. En algunos ejemplos (guerras de hackers entre Corea del Norte y del Sur; intentos rusos de socavar la OTAN, las intrigas permanentes del Ejército Electrónico Sirio, etc.), las evidencias parecen confirmar que se utilizaron los métodos hacktivistas, ya como una cortina de humo, ya empleados directamente por agentes de los Estados-nación, como herramientas de información en conflictos geopolíticos.

Event or Campaign	Hacktivist Group Attribution	Suspected State Involvement	State Objectives Served
OpAbabil	Izz Ad-din Al-Qassam Cyber Fighters (AQCF)	Directed by Iranian state	US financial infrastructure computer network disruption
2013 SEA Activity	SEA	Executed by Syrian military or state	Psychological operations and cyber-force projection or deterrence
OpNorthKorea	High Anonymous*	Integrated by North Korean state	South Korea critical information infrastructure disruption
OpIndependence	Anonymous Ukraine*	Created by Russian state	Psychological operations and undermining NATO cyber-capability

Mientras que el hacktivismo se ha usado como tapadera para las operaciones patrocinadas por los Estados contra redes de ordenadores, por lo menos desde los atentados -atribuidos a Rusia- en Georgia y Estonia en 2007 y 2008, el uso de tácticas, técnicas y procedimientos (TTP) de estilo hacktivista en el contexto de conflictos geopolíticos se produjo en tal medida en 2013 que constituyó uno de los rasgos definitorios del panorama de las ciberamenazas de este año. Algunos ejemplos clave son la continuación de la Operación Ababil (**OpAbabil**) en 2013, el incremento de la actividad maliciosa atribuida al **SEA**, los ataques recíprocos entre Corea del Norte y del Sur durante OpNorthKorea -que se atribuyeron inicialmente a un grupo de hacktivistas de Corea del Norte-, y el potencial uso de Rusia de entidades hacktivistas en el contexto de la inestabilidad política ucraniana durante el otoño. Tomados en su conjunto, estos ejemplos son referente de un fenómeno que se ha venido desarrollando desde hace varios años: los Estados explotan la percepción pública y mediática de la actividad de estilo hacktivista para justificar acciones que responden a motivos concretos y definidos.

Generalmente, el hacktivismo se ha venido manifestando mediante ataques DDoS, revelación de información personal identificable y desfiguraciones de páginas web, tipos de

ataque todos ellos que, pese a no ser exclusivos del hacktivismo, suelen estar popularmente vinculados a él. Sin embargo, lo que los actores de los Estados parecen aprovechar es el hecho de que los TTP hacktivistas son bastante difíciles de aislar de otras categorías de comportamiento dañino online. Lo que hace distinto al hacktivismo se relaciona con la intención, y ésta es difícil de determinar en la mayoría de los casos. Los grupos hacktivistas, a diferencia de los agentes de los Estados, suelen comunicar de forma transparente sus intenciones antes o al mismo tiempo de producirse un ataque, como en el caso de los miembros del movimiento GreenRights durante el ataque a Monsanto Corporation, donde perseguían dañar su reputación por el uso de organismos modificados genéticamente por parte de la empresa.

En los casos mencionados anteriormente, hay evidencias de que los Estados en cuestión o sus representantes estaban utilizando este modelo de ataques con el objeto de engañar o simplemente confundir los intentos de atribuir la actividad maliciosa a un actor concreto. El caso de OpAbabil es el más claro ejemplo de este fenómeno.

Un ejemplo muy significativo de los TTP hacktivistas en acciones al servicio de intereses de Estado, se produjo en 2013, en el contexto de la tensión ucraniana en torno a la relación de este país con la UE, la OTAN y Rusia. A finales de octubre, una entidad que se autodenominaba Anonymous Ukraine perpetró una serie de ataques bajo la llamada OpIndependence. Anonymous Ukraine lanzó sus ataques contra dominios de Polonia, Estonia, Ucrania, la UE y el Cooperative Cyber Defence Centre of Excellence (CCD-CoE) de la OTAN, motivado por el deseo de socavar el ejercicio militar conjunto de la OTAN denominado "Steadfast Jazz".

Basado en el análisis que los investigadores llevaron a cabo en los correos de spam que supuestos "miembros de Anonymous Ukraine" habían remitido y la correlación entre las IP desde la que se enviaron las diferentes comunicaciones, se cree que la entidad Anonymous Ukraine estaba siendo administrada por un abonado de Caucasus Online LLC ASDL en Georgia, un ISP con frecuencia vinculado en actividades de botnets. Por su integración y enfoque estas acciones parecen beneficiar al Gobierno ruso.

Rusia tiende a un enfoque integral de la ciberseguridad, el ciberespionaje, las comunicaciones y la opinión pública, sobre todo en la "esfera político-militar", lo que implica la "integración de la fuerza militar, las capacidades no militares y el papel de la guerra de información"[77].

6.4 Riesgos en crecimiento

6.4.1 Los ataques por *Watering Hole*, Descentralización, DDoS y ataques DNS

Un tipo de ataque relativamente reciente es el llamado ataque por *Watering Hole*. En 2013, se han comprometido varias organizaciones relacionadas con la tecnología[78], colocando exploits en determinadas páginas web que algunos los empleados de la organización objetivo

77 "Военная доктрина Российской Федерации: Указ Президента Российской Федерации" ("Military Doctrine of the Russian Federation, Declaration of the President of the Russian Federation"). Feb. 10, 2010. kremlin.ru. http://news.kremlin.ru/ref_notes/461.

78 http://threatpost.com/why-watering-hole-attacks-work-032013/77647

solían visitar con frecuencia. Tales exploits propiciaron la instalación de código dañino en los ordenadores de los visitantes. Esta misma metodología también ha sido usada para atacar a empleados públicos[79].

Este tipo de ataques puede alcanzar a un importante número de objetivos, comprometiendo un único lugar. Usando esta técnica, se han atacado las páginas web de varios sitios importantes de alto tráfico, tales como Los Angeles Times, el National Journal, Toyota Japón, y MSI Electronics. En junio, los creadores del navegador Opera informaron de haber sufrido un ciberataque que comprometió, al menos, a uno de sus certificados de firma de código. Este incidente supuso que, durante un periodo de tiempo, las personas que pensaban que estaban descargando una versión legítima -debidamente firmada- de software, podían haber estado descargado código dañino.

2013 fue igualmente testigo de ataques contra delegaciones regionales (ataques por Descentralización) de grandes empresas y corporaciones. Con frecuencia, estas organizaciones, no siempre adoptan el mismo nivel de seguridad en estos emplazamientos que en la sede central. Varias empresas sufrieron daños relacionados con su reputación, y tuvieron que hacer frente a importantes implicaciones legales relacionadas con la exfiltración grandes cantidades de datos de clientes. Este tipo de fugas afectaron singularmente a empresas de los sectores de la alimentación, la electrónica de consumo, la automoción y las industrias del entretenimiento[80].

Otros incidentes de seguridad de 2013 han sido provocados por ataques DDoS contra grandes organizaciones. El sector financiero sufrió ataques de este tipo que provocaron que los servicios de banca online permanecieran inactivos durante periodos de tiempo significativos.

Spamhaus[81], una organización sin ánimo de lucro y dedicada al seguimiento del spam, fue atacada con lo que algunos consideran el mayor ataque DDoS de la historia, con tasas de tráfico registrado de hasta 300 Gbps.

Estos ataques DDoS de banda ancha aumentaron significativamente durante 2013, constituyendo un verdadero desafío para todas las organizaciones (públicas o privadas) que sostienen servicios online o desarrollan servicios de administración electrónica. Por otro lado, no hay que olvidar que estos ataques DDoS también pueden obedecer a maniobras de distracción de ataques de mayor calado.

Finalmente, una nueva tendencia es la perpetración de ataques contra proveedores DNS a través de ataques DDoS, tendencia que se ha venido observando desde junio de 2013, que

79 http://news.softpedia.com/news/Cybercriminals-Behind-DOL-Watering-Hole-Attack-Target-USAID-Employees-353138.shtml

80 http://www.cyberwarnews.info/2013/07/13/sony-italy-hacked-over-40k-personal-details-leaked/
http://www.cyberwarnews.info/2013/06/20/samsung-kazakhstan-social-hub-domain-hacked-62235-accounts-leaked/
http://www.cyberwarnews.info/2013/08/22/fast-food-giant-pizza-hut-spain-and-malta-hacked-data-leaked-site-redirected/
http://www.cyberwarnews.info/2013/03/31/official-mtv-taiwan-hacked-607286-account-credentials-leaked/
http://www.cyberwarnews.info/2013/03/28/official-mcdonalds-austria-taiwan-korea-hacked-over-200k-credentials-leaked/

81 http://www.informationweek.com/security/attacks/spamhaus-ddos-suspect-arrested/240153788

han sufrido interrupciones del servicio[82]. Seleccionar como víctimas a los proveedores de servicios DNS permite alcanzar un mayor número posible de víctimas potenciales. Así, si un proveedor de DNS permanece inaccesible debido a un ataque DDoS, cualquier sitio cuyo dominio dependa de éste se verá igualmente afectado[83]. Por otro lado, si los atacantes pueden infectar al proveedor de DNS usando DNS-Hijacking[84], podrían redirigir las direcciones web a servidores alternativos, que podrían utilizarse, a su vez, para desarrollar ataques de phishing o distribución de código dañino.

6.4.2 Los riesgos derivados de la autenticación de un factor

El modelo de autenticación de un único factor está llamado a desaparecer. En la actualidad, pueden descargarse de Internet herramientas capaces de romper una contraseña simple en pocos segundos. Las credenciales almacenadas en bases de datos (accesibles a través de portales web e inyección SQL), junto con las relacionadas con seguridad inalámbrica (WPA2) constituyan objetivos habituales.

Se hace necesario, por tanto, evolucionar hacia mecanismos de autenticación de varios factores, tanto para los usuarios internos de los sistemas de información de las organizaciones, como para los externos, clientes o ciudadanos. Además de la autenticación basada en certificados digitales, el segundo factor puede consistir en remitir al usuario -a través, por ejemplo, de dispositivos móviles-, una segunda contraseña de un solo uso. No obstante, pese a que, como se ha evidenciado durante 2013, esta doble autenticación no es la panacea[85], las garantías adicionales que comporta están haciendo que sean mecanismos cada vez más utilizados86.

6.4.3 Ataques contra comunicaciones Máquina-a-Máquina (M2M)

Como es sabido, la comunicación Máquina-a-Máquina (M2M) hace referencia a aquellas tecnologías que permiten a los sistemas, de forma cableada o inalámbrica, la comunicación automática con otros dispositivos que posean la misma capacidad[87].

Durante 2013 se han evidenciado los primeros ataques dirigidos a interceptar y alterar este tipo de comunicaciones entre máquinas. Un ejemplo de estos ataques tuvo lugar en junio de 2013, cuando la FDA[88] y el ICS-CERT[89] alertaron sobre posibles problemas de este tipo con ciertos dispositivos de naturaleza médica, tales como marcapasos, bombas de insulina y desfibriladores.

82 http://www.pcworld.com/article/2040766/possibly-related-ddos-attacks-cause-dns-hosting-outages.html

83 http://www.theregister.co.uk/2013/07/18/netsol_ddos/

84 http://www.zdnet.com/linkedin-just-one-of-thousands-of-sites-hit-by-dns-issue-cisco-7000017124/

85 Como así se ha podido ver con el botnet Zitmo, capaz de romper la autenticación dos factores en dispositivos Android, y la brecha del token de seguridad SecurID de RSA durante 2011.

86 Tales como Twitter, Outlook.com, Dropbox, Evernote y Facebook, entre otros.

87 Se trata de una de las características de lo que se ha dado en llamar "Internet of Things".

88 US Food and Drug Administration. (www.fda.gov)

89 www.ics-cert.us-cert.gov

6.4.4 La capacidad de los exploits para eludir los sandbox

El sandbox es una tecnología de seguridad que se emplea frecuentemente para separar los programas y aplicaciones en ejecución, de forma que el código dañino no pueda transferirse de un proceso a otro. En la actualidad, varios proveedores de software, tales como Adobe y Apple, están usando este mecanismo que, durante 2013, ya se ha visto comprometido por algunos exploits capaces de eludir máquinas virtuales y entornos aislados. Entre ellos están las vulnerabilidades detectadas para Adobe Reader[90]. Es muy probable que, durante 2014, se detecte código dañino con esta funcionalidad.

6.4.5 Botnets para plataformas cruzadas

Durante 2013 se han encontrado botnets para dispositivos móviles que poseen muchas de las características y funcionalidades tradicionalmente empleadas por los atacantes en el diseño y desarrollo de botnets para ordenadores personales. Siguiendo con esta tendencia, durante 2013 se han detectado nuevas formas de ataques DDoS que pueden surgir tanto desde equipos PC como desde dispositivos móviles. Por ejemplo, un dispositivo móvil infectado y un PC pueden compartir el mismo servidor de mando y control (C&C) y el protocolo de ataque, actuando, por tanto, de manera sincronizada.

Análogamente, durante 2013 se han reportado evidencias de código dañino diseñado para Android que también ha intentado infectar ordenadores con SO Windows, en el momento de la sincronización de ambos dispositivos.

6.4.6 El crecimiento de código dañino para dispositivos móviles

En la actualidad, el desarrollo de código dañino tiene como objetivo tanto a los dispositivos móviles como a los ordenadores portátiles o de sobremesa. Históricamente, sin embargo, los mayores esfuerzos de desarrollo se habían dirigido a los PC, porque el parque de este tipo de equipos era significativamente mayor que el resto. Esto hacía que, frente a los millones de ejemplos de código dañino para PC, existieran tan sólo unas pocas decenas de miles para dispositivos móviles.

Durante 2012 y 2013 se ha asistido a un importante incremento del volumen del código dañino dirigido a dispositivos móviles, debido especialmente al incremento exponencial en su uso y al reducido número de defensas que, todavía en la actualidad, tienen este tipo de equipos.

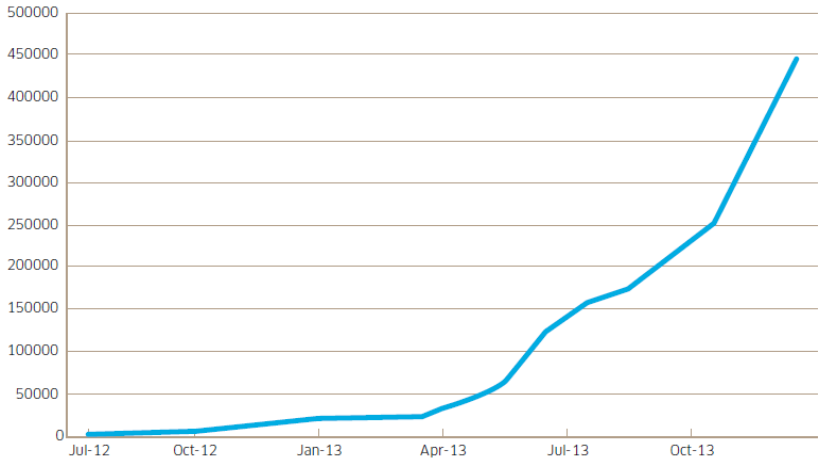
A finales de 2013, había 11,6 millones de dispositivos móviles infectados en todo el mundo, habiendo crecido la tasa de infección en 2013 en torno al 20%, y siendo los dispositivos LTE[91] los más proclives a ser infectados.

90 Como así fue evidenciado por el grupo polaco Security Explorations, en abril de 2013, lo que obligó a Adobe a parchear su software Reader.

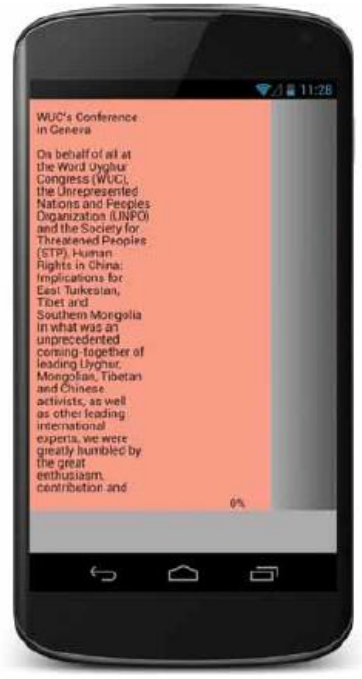
91 LTE es un acrónimo de Long Term Evolution, conocido habitualmente en el Mercado como 4G-LTE, es un estándar para comunicaciones inalámbricas de datos a alta velocidad, para teléfonos móviles y terminales de datos.

Por lo que respecta a los sistemas operativos de los dispositivos móviles, según distintos estudios[92], Android opera en la actualidad en el 59% de todos los dispositivos móviles inteligentes. En 2012 se habían vendido más de 470 millones de dispositivos Android y, si los pronósticos que estamos manejando[93] son exactos, para el año 2017 habrá más de mil millones de dispositivos Android en uso. Correlativamente, este aumento ha generado homóloga atención por parte de los autores de código dañino.

El gráfico de la figura siguiente muestra la evolución de código dañino para Android durante la segunda mitad de 2012 y 2013.



Por ejemplo, el código dañino *Chuli*, descubierto en marzo de 2013, fue utilizado para un dispositivo móvil de un supuesto hacktivista tibetano. Usando la cuenta atacada, se remitían correos electrónicos a los contactos del dispositivo, pretendiendo ser asistentes al "Congreso Mundial Uygur". El archivo adjunto era un APK de Android llamado "WC's Conference.apk". Cuando se abría, *Chuli* mostraba un mensaje inocuo relativo a la conferencia. Sin embargo, el código dañino se introducía en el servicio SMS de Android para interceptar los mensajes SMS entrantes, remitiéndolos a un C&C. Además, se remitía el historial de navegación del usuario, relación de llamadas, contactos y geolocalización.



92 http://www.canalys.com/newsroom/smart-mobile-device-shipments-exceed-300-million-q1-2013

93 http://www.canalys.com/newsroom/over-1-billion-android-based-smart-phones-ship-2017

La existencia de este tipo de código dañino indica que los usuarios de Android constituyen objetivos cada vez más viables para este tipo de ataques.

El que, durante el pasado año, fue considerado el código dañino más sofisticado para Android –Obad-, alcanzó su máxima relevancia en junio de 2013[94]. Aunque la funcionalidad principal de Obad ya se había observado previamente en otros tipos de código dañino Android, incluyendo el robo de información y el envío de SMS Premium, se enumeran seguidamente algunas de sus características más significativas:

<table>
<tr>
<td>1. Técnicas anti-análisis y de ofuscación de código

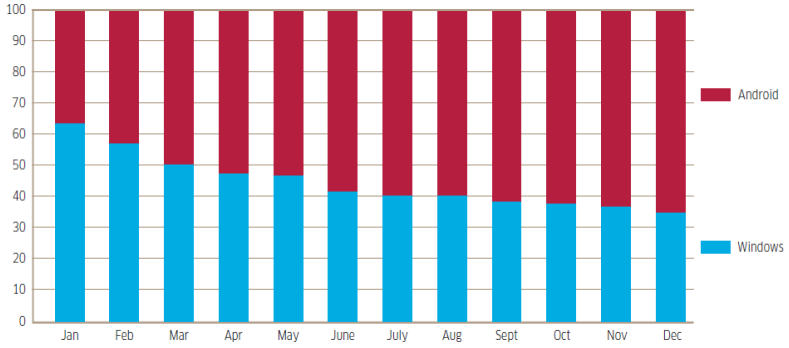
Obad emplea dos exploits que hacen más difícil el análisis, tanto estático como dinámico. En primer lugar, modifica el ejecutable Dalvik en el APK, de forma que provoca un error en algunas herramientas de ingeniería inversa. En segundo lugar, también altera *AndroidManifest.xml,* incluido en el APK.
Obad, además, utiliza ofuscación de código para hacer más difícil su análisis. Todas las cadenas (*strings*), incluyendo los nombres de clases y métodos, se cifran. Para hacer aún más difícil el análisis incorpora código basura.</td>
<td>2. Administración de dispositivos

Cuando se instala *Obad*, se pide al usuario privilegios de administrador, lo que le otorga ciertas potestades tales como el bloqueo del dispositivo. También evita que la aplicación se desinstale de la manera normal. Para desinstalar una aplicación de administrador de dispositivos, el usuario tiene que desinstalarlo a través de la lista del Administrador en el menú *Ajustes*. Sin embargo, *Obad* explota un bug en Android que impide a una aplicación estar registrada en la lista del Administrador, lo que impide su eliminación.</td>
</tr>
<tr>
<td colspan="2">3. Difundirse a través de Bluetooth

Otra característica única de *Obad* es su capacidad para propagarse a través de Bluetooth. El código puede recibir un comando desde el servidor C&C, indicándole que debe buscar dispositivos Bluetooth habilitados en los alrededores a los que, seguidamente, intentará remitir un archivo dañino.</td>
</tr>
</table>

A pesar del importante aumento en el número y la sofisticación de código dañino para Android, todavía no ha alcanzado el nivel de sofisticación de sus homólogos para Windows PC. La figura siguiente muestra la evolución de código dañino para Android en comparación con el equivalente de Windows PC.

94 http://www.securelist.com/en/blog/8106/The_most_sophisticated_Android_Trojan



6.4.7 El *ramsonware* ataca a los dispositivos móviles

Durante 2013, el tipo de código dañino conocido como *ramsonware* (una infección que "secuestra" el dispositivo de la víctima hasta que se satisface un "rescate") ha empezado a migrar desde los PCs a los dispositivos móviles.

Así, durante la primera mitad de 2013, el código dañino FakeDefender[95] comenzó a atacar dispositivos Android. FakeDefender instaba a las víctimas a comprar un falso antivirus para limpiar las infecciones detectadas. Seis horas después de que el código dañino se instalaba en el dispositivo en cuestión, lo bloqueaba con una imagen pornográfica y un enlace dirigido a comprar el software que limpiaría el dispositivo de la infección. Además, el código dañino buscaba en el dispositivo ficheros clave y los borraba, evitando con ello la restauración del equipo desde un fichero de backup.

6.4.8 BYOD, Cloud Computing y Redes Sociales

Los riesgos derivados del uso de estos modelos, pese a no ser nuevos, también evolucionan a medida que lo hacen las tecnologías que los soportan y los hábitos de los usuarios. Cada uno de ellos es único en sus implicaciones de seguridad.

La figura siguiente muestra el grado de importancia que les confieren los responsables de la seguridad IT de algunas organizaciones norteamericanas, publicado en un reciente estudio[96].

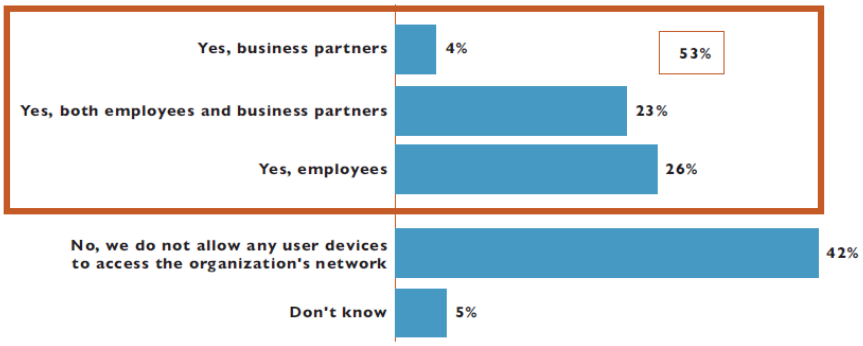
95 Código dañino que se hace pasar por un antivirus.

96 Frost & Sullivan, op. cit.

Hasta hace relativamente muy poco tiempo, el modelo BYOD (Bring Your Own Device) no constituía un peligro real. Los usuarios usaban el ordenador que le había sido suministrado por la organización, y si un empleado tenía necesidad de acceso al correo electrónico, se le proporcionaba un módem para su ordenador portátil o un smartphone institucional, generalmente un dispositivo del tipo Blackberry.

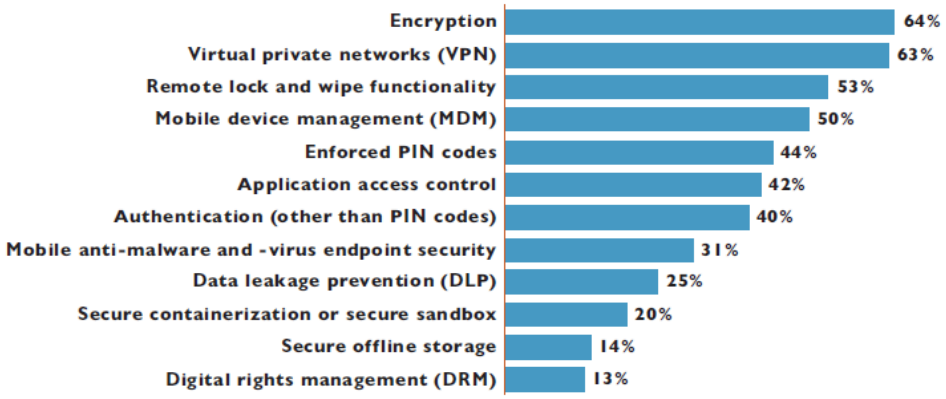
En actualidad, BYOD es una modalidad de trabajo que ha sido adoptada por muchas compañías e instituciones públicas. Los empleados, especialmente trabajadores jóvenes, han venido demandando la posibilidad de usar sus propios dispositivos en su trabajo habitual. El incremento de productividad ha alentado a las organizaciones a adoptar esta estrategia.

La figura siguiente muestra la utilización del modelo BYOD en EE.UU. encuestadas en el antedicho estudio.



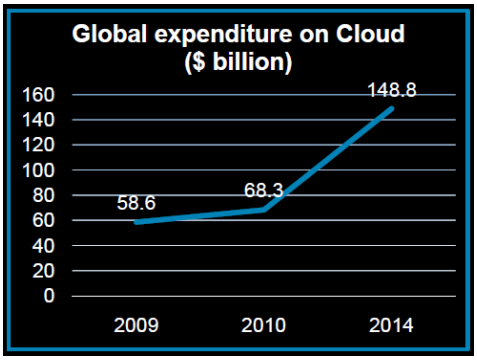
No obstante, como es sabido, este modelo tiene sus riesgos; esencialmente los derivados de la posibilidad de que la información corporativa pueda filtrarse a los dispositivos de los empleados, sin ningún control. Por tanto, ya no se trata de que los atacantes consigan lograr acceso a la tarjeta SIM de los dispositivos móviles y, con ello, generar llamadas fraudulentas, sino que el peligro radica en el uso de los dispositivos personales como mecanismo para acceder a datos de naturaleza corporativa.

Atendiendo a los datos revelados por la encuesta antedicha, la figura siguiente muestra las tecnologías de seguridad más usadas cuando se utiliza el modelo BYOD.



Por otro lado, todos los estudios consultados confirman el creciente uso de los **servicios en la nube** (*Cloud Computing*), especialmente entre las grandes organizaciones.

La figura muestra la evolución de las estimaciones de gasto de las organizaciones en tecnología Cloud.



La selección entre las diferentes modalidades de uso de Cloud Computing se corresponde con el nivel de riesgo que las organizaciones son capaces de asumir[97]. Como se muestra en la tabla siguiente, los servicios de cloud computing privados –donde el cliente conserva un mayor control sobre la infraestructura de nube y la securización de tal infraestructura- son, proporcionalmente, los más usados[98].

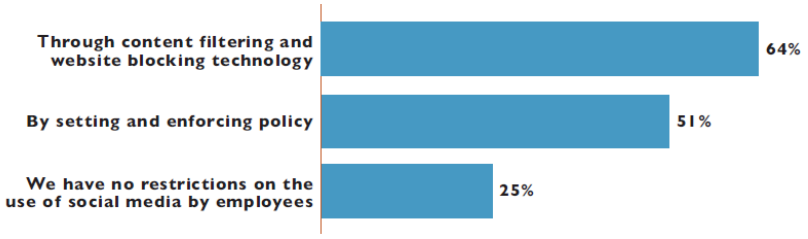
97 Véase Guía CCN-STIC 823: Seguridad en Cloud Computing.

98 Fuente: Frost & Sullivan 2013 Global Information security Workforce

	Proportionate Use of Cloud Computing Approaches — Current						
	Total Survey	Banking, Insurance & Finance	Education	Healthcare	Info Tech	Telecom & Media	Gov't
Private cloud computing services	38%	41%	37%	38%	34%	37%	46%
Software as a Service	19%	22%	19%	25%	19%	15%	13%
Infrastructure as a Service	11%	11%	7%	8%	12%	13%	11%
Public cloud computing services	11%	8%	16%	10%	11%	12%	9%
Platform as a Service	7%	7%	5%	6%	8%	9%	7%
Hybrid cloud computing services	7%	6%	7%	7%	8%	8%	8%
Community cloud computing services	6%	4%	9%	6%	6%	6%	6%

Por último, aunque los problemas de seguridad asociados al uso de las **Redes Sociales** suelen ser percibidos como menores en relación con el BYOD y el Cloud Computing, no es menos cierto que las organizaciones (públicas y privadas) están empezando a adoptar medidas para gestionar el riesgo que emana del uso de tales redes, especialmente aquellas relativas a limitar su acceso y el filtrado y bloqueo de contenidos.

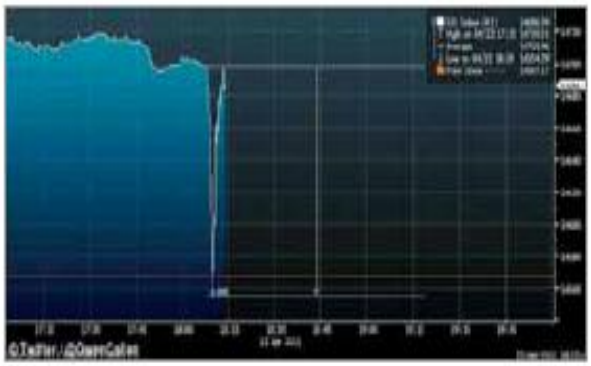
La figura siguiente muestra las limitaciones más frecuentes entre los usuarios de las organizaciones cuando pretenden acceder a redes sociales.



Como quiera que la utilización de las redes sociales, tanto por parte de las personas individuales como de las organizaciones, al objeto de darse a conocer o promover la venta de productos o la prestación de servicios, se ha convertido en una actividad irrenunciable, bloquear el acceso no parece una solución idónea, lo que está provocando que se estudien distintas posibilidades para monitorizar su uso.

Un ejemplo palmario: en abril de 2013, los sesenta caracteres de un solo tweet le cuestan al mercado de valores de EE.UU. 200 mil millones de dólares[99]. Este incidente pone de manifiesto la confianza que las redes sociales despiertan en el público cuando la información compartida proviene de una fuente que se reputa fiable.

99 El "flash crash" tuvo lugar cuando la cuenta de noticias de Twitter de Associated Press sufrió un ataque en el que sus autores escribieron: "Últimas noticias: Se han producido dos explosiones en la Casa Blanca. Barack Obama está herido."



Associated Press no fue la única gran organización que, en 2013, perdió el control de su cuenta en las redes sociales. El canal de Reuters en Twitter[100] fue atacado por el Ejército Electrónico Sirio (SEA), utilizándose para publicar caricaturas políticas apoyando al presidente sirio, Bashar al-Assad. Como hemos referido antes, eL SEA comprometió también la página de Facebook, del diario New York Post[101,] y las de Twitter de algunos de sus periodistas, así como la cuenta de The Onion[102], donde publicaron 26 tweets denunciando a Israel y a los EE.UU.

Por su parte, Anonymous, comprometió la cuenta de Burger King en Twitter103, utilizando el ataque para promover a su competidor: McDonalds. Al día siguiente, la cuenta Twitter de Jeep fue atacada, afirmándose que Jeep se había vendido a Cadillac[104.]

Como es lógico suponer, el valor de poseer una cuenta reputada en una red social ha desarrollado un mercado negro[105] en el que los actores dañinos se dedican a vender cuentas comprometidas o cuentas diseñadas y creadas para dar la apariencia de ser cuentas fiables y reales.

Pese a sus riesgos, las redes sociales siguen constituyendo una plataforma de comunicación clave para las organizaciones de todo el mundo. Por ello, es necesario que los usuarios de las cuentas de tales redes conozcan las medidas de seguridad que deben adoptar en cada momento.

100 http://www.theguardian.com/technology/2013/jul/30/reuters-twitter-hacked-syrian-electronic-army

101 http://www.thedailybeast.com/articles/2013/08/13/syrian-electronic-army-strikes-again-hits-socialflow-new-york- post.html

102 http://arstechnica.com/security/2013/05/no-joke-the-onion-tells-how-syrian-electronic-army-hacked-its-twitter/

103 http://www.telegraph.co.uk/technology/twitter/9878724/Burger-Kings-Twitter-account-hacked.html

104 http://www.huffingtonpost.com/2013/02/19/jeep-twitter-hack_n_2718653.html

105 http://blog.webroot.com/2013/06/07/hacked-origin-uplay-hulu-plus-netflix-spotify-skype-twitter-instagram-tumblr-freelancer-accounts-offered-for-sale/

6.4.9 Actualización de botnets para dispositivos móviles

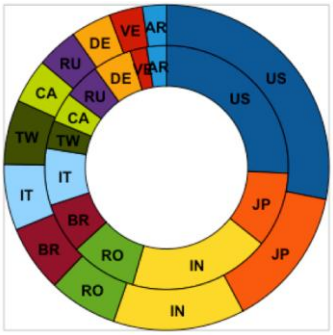
ZeroAccess

En abril de 2013 se evidenció que los autores de la botnet ZeroAccess estaban invirtiendo importantes cantidades de dinero en mantener la penetración de su código dañino. Ese mismo mes se detectaban, como media, 100.000 nuevas infecciones semanales[106].

Los desarrolladores de ZeroAccess crearon nuevas versiones de código dañino, de forma que, en la actualidad, podemos afirmar que existen cuatro bots ZeroAccess en operación, de 32 y 64 bits, dirigidas al fraude del click (click fraud) y a explotar Bitcoin, lo que evidencia que las personas que están detrás de estas botnets persiguen infectar el mayor número posible de dispositivos y seguir generando ingresos.

Pese a que ZeroAccess es una botnet global, los Estados Unidos continúan teniendo el mayor número de infecciones, aunque se ha detectado un importante número de ellas en Japón, India, Rumanía, Brasil, Italia, Taiwán, Canadá, Rusia, Alemania, Venezuela y Argentina.

La figura siguiente muestra la penetración de esta amenaza desde enero (anillo interior) a junio de 2013.



Citadel

En junio de 2013, Microsoft, en colaboración con el FBI y los tribunales de los Estados Unidos, asestaron un duro golpe a las capacidades de esta botnet.

Como es sabido, Citadel es una variante de ZeuS responsable de infectar millones de ordenadores en todo el mundo, sustrayendo información financiera a través de key logging, así como dinero de las cuentas bancarias de las víctimas.

La operación conjunta, denominada Operation B54, logró desactivar simultáneamente el funcionamiento de 1.400 botnets. Evidentemente, esta operación, aun habiendo sido un éxito, no logró desmontar completamente la botnet, por lo que es de esperar que sus autores desarrollen nuevas versiones para reemplazar las que han sido detectadas.

106 Fuente: Fortinet: April Threat Landscape Report.

6.4.10 Otros riesgos en crecimiento

Ejecución remota de código *Ruby on Rails*

Ruby on Rails (RoR) es un entorno de desarrollo de aplicaciones web para el lenguaje de programación Ruby, permitiendo un despliegue rápido y fácil de sitios web "Web 2.0". RoR es una infraestructura muy popular en cientos de miles de sitios web.

En enero de 2013, se anunció que una vulnerabilidad crítica en RoR que podría dar a un atacante remoto la posibilidad de ejecutar código en el servidor Web subyacente. Aunque fue parcheado para corregir el defecto, siguen existiendo sitios web sin actualizar.

Estas vulnerabilidades en entornos de desarrollo web son de gran utilidad para realizar ataques posteriores como Watering Hole.

Ejecución remota de código Java

En enero de 2013, un exploit de día-cero fue capaz de eludir el sandbox de Java y ejecutar código Java dañino.

Como es sabido, Java es una tecnología ubicua, la mayoría de los ordenadores tienen Java instalado y activo. La vulnerabilidad mencionada permite a un programa dañino ejecutar cualquier software, eludiendo el sandbox de Java y permitiendo un acceso total al equipo atacado.

El exploit se integró rápidamente en muchos kits de software dañino[107], otorgando a los compradores de tal software la posibilidad de explotar las vulnerabilidades e instalar código dañino en los ordenadores de las víctimas. El exploit utilizó un defecto en un componente JMX (Java Management Extensions) que permitía al applet dañino elevar sus privilegios y ejecutar cualquier código Java.

Oracle se apresuró a lanzar un parche para esta brecha de seguridad, aunque todavía se siguen encontrando muchos ordenadores que no han actualizado sus versiones de Java.

Exploit zero-day para Acrobat y Acrobat Reader

En febrero de 2013, se detectó un PDF que, pretendiendo ser una forma de visado de viaje de Turquía, aprovechaba una vulnerabilidad inédita en Adobe Reader. El exploit funcionaba con todas las versiones recientes de Adobe Reader (9.5.X, 10.1.X y 11.0.X) y en la mayoría de versiones de Microsoft Windows, incluyendo Windows 7 de 64 bits, así como en la mayoría de los sistemas Mac OS X.

Como en otras ocasiones, el exploit de PDF fue utilizado por los atacantes para instalar código dañino en los ordenadores objetivo.

Adobe lanzó un parche el 20 de febrero, pero todavía en la actualidad se siguen utilizando versiones de este exploit, en ataques con correos dirigidos.

107 Tales como BlackHole, Redkit y Pack Nuclear.

Ataques DDoS masivos en Spamhaus

En abril de 2013, a través de diversas botnets se lanzó un ataque de denegación de servicio distribuida (DDoS) contra CloudFlare y otros proveedores de infraestructuras de Internet (que alojan el proyecto Spamhaus).

Este proyecto Spamhaus provee servicios de listas negras para muchos proveedores de Internet y servidores de correo electrónico de todo el mundo, con la intención de detener los miles de millones de mensajes de spam enviados diariamente. En febrero de 2013, se incluyó al proveedor de alojamiento holandés CyberBunker en su lista negra. En represalia, se realizó el citado ataque. Se señalaron como posibles responsables a una alianza de hacktivistas y ciberdelincuentes, conocida como Proyecto STOPhaus.

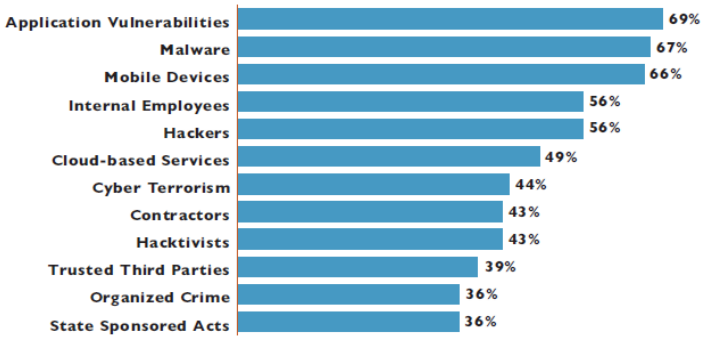
CDorked ataca Apache

A finales de abril de 2013, se evidenció un nuevo ataque contra el popular servidor web Apache empleando el código dañino CDorked que era capaz de comprometer el servidor web atacado y redirigir a los visitantes a otros servidores que infectaban a la víctima utilizando el exploit kit BlackHole. El ataque también podía tener como objetivo a los servidores web Lighttpd y Nginx.

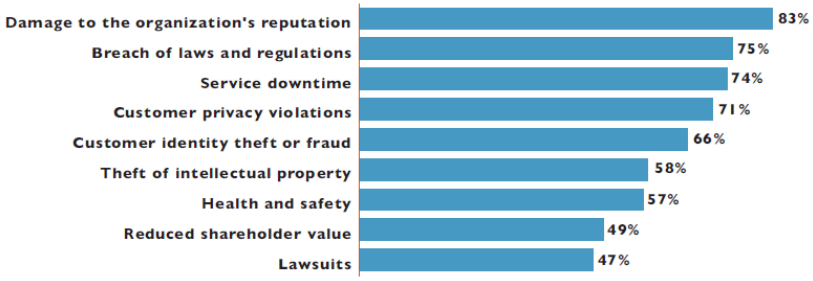
CDorked presentaba muchas similitudes con el ataque de DarkLeech de 2012 contra servidores Apache, aunque es mucho más sigiloso y sofisticado.

7. ANÁLISIS DE LAS AMENAZAS GENERALES

Como se ha señalado repetidamente, las amenazas y las vulnerabilidades a las que deben enfrentarse los profesionales de la ciberseguridad, tanto del sector público como del privado, son muy amplias. La figura siguiente muestra aquellas que han sido consideradas como más importantes en una reciente encuesta dirigida a los profesionales de la seguridad IT en los EE.UU.[108].



La figura siguiente muestra el orden de importancia por tipo de impacto.



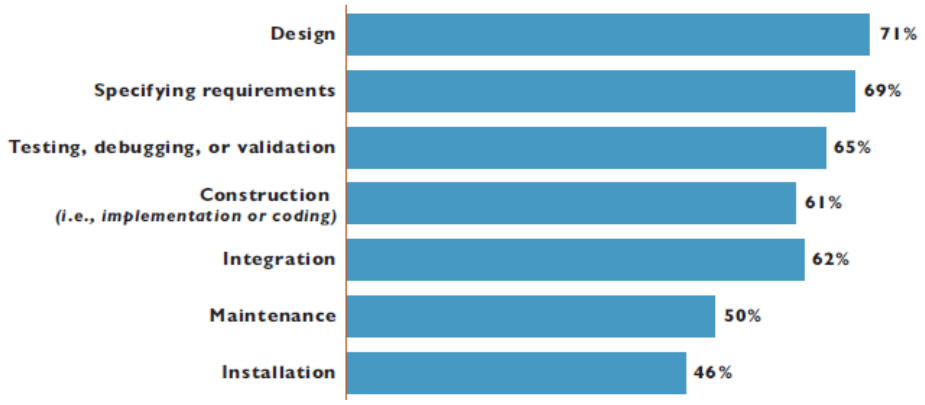
Se hace seguidamente un repaso de las amenazas generales más significativas halladas en los incidentes de ciberseguridad en 2013.

7.1 Vulnerabilidades

Como es sabido, las vulnerabilidades son debilidades en el software que permiten a un atacante comprometer la integridad, disponibilidad o confidencialidad del propio software o de los datos que procesa. Algunas de las vulnerabilidades más peligrosas permiten a los atacantes ejecutar código dañino en el sistema comprometido.

Los riesgos derivados de las vulnerabilidades del software afectan a múltiples fases del ciclo de vida del software, desde su desarrollo a la instalación o mantenimiento, tal y como muestra la figura siguiente, atendiendo a los datos de la encuesta mencionada anteriormente.

108 Frost&Sullivan: 2013 Global Information Security Work Force

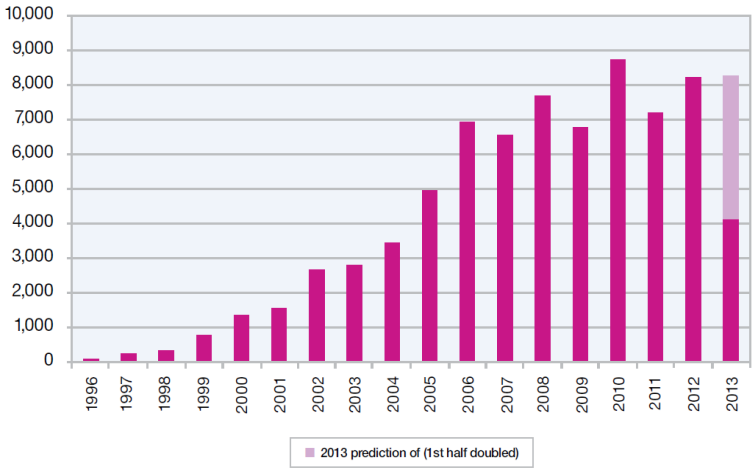


7.1.1 Divulgación de vulnerabilidades

Una divulgación es la revelación pública de una vulnerabilidad software. Tales revelaciones pueden provenir de una multiplicidad de fuentes, incluyendo los fabricantes del software afectado, los proveedores de software de seguridad, los investigadores de seguridad independientes e, incluso, los propios creadores de código dañino.

La información de este epígrafe es una recopilación de datos de divulgación de vulnerabilidades que se publica en la National Vulnerability Database (NVD) de los EE.UU. que contiene datos de todas las vulnerabilidades publicadas[109]. A estas se les asigna un identificador CVE (Common Vulnerabilities and Exposures)[110].

En el primer semestre de 2013, se notificaron algo más de 4.100 nuevas vulnerabilidades de seguridad. La figura siguiente muestra la evolución de las vulnerabilidades en los dos últimos años[111].



109 http://nvd.nist.gov/

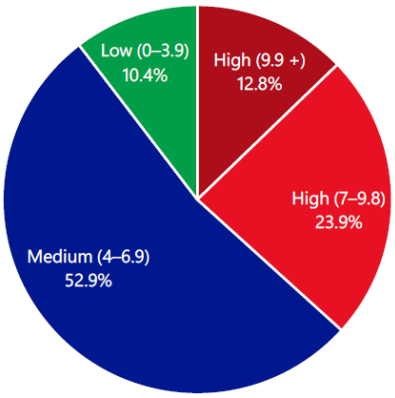
110 Las entradas de CVE están sujetas a una permanente revisión, tanto de los proveedores de software como de los investigadores de seguridad. Por esta razón, las estadísticas mostradas en este documento pueden diferir ligeramente de estadísticas con un diferente grado de actualización.

111 Fuente: IBM X-Force Mid Year Trend and Risk Report 2013.

7.1.2 La gravedad de las vulnerabilidades

El Common Vulnerability Scoring System (CVSS) es un sistema normalizado de valoración, independiente de la plataforma, que permite asignar a las vulnerabilidades TIC[112] un valor numérico, entre 0 y 10, atendiendo a su gravedad[113].

La figura siguiente muestra el desglose de vulnerabilidades, por severidad.



Divulgación de vulnerabilidades en 1H13, por gravedad

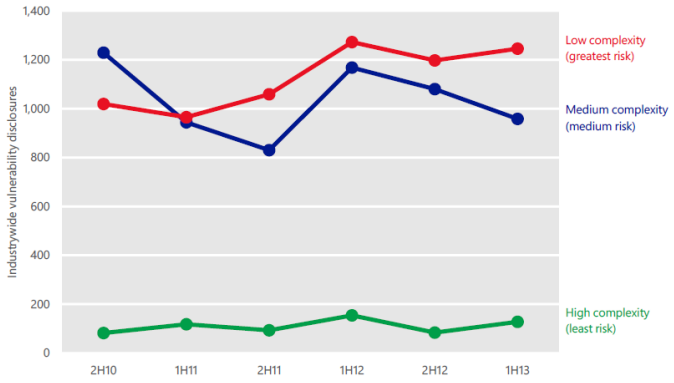
7.1.3 La complejidad de las vulnerabilidades

La complejidad de la vulnerabilidades (lo que está en relación con la mayor o menor facilidad con la que pueden ser explotadas) es un factor decisivo a la hora de determinar la magnitud del riesgo. En otras palabras: una vulnerabilidad grave que sólo pueda explotarse en circunstancias muy específicas o poco frecuentes exige una menor atención que una vulnerabilidad de menor gravedad que pueda ser explotada con mayor facilidad.

El CVSS asigna a cada vulnerabilidad un ratio de complejidad del tipo: Low (Baja), Medium (Media) o High (Alta). La figura siguiente muestra la complejidad de las vulnerabilidades divulgadas desde el segundo semestre de 2010. Recordemos que una complejidad Low (Baja) implica un mayor riesgo.

112 http://www.first.org/cvss

113 Definición adaptada de: http://www.microsoft.com/security/sir/glossary/vulnerability-severity.aspx



Divulgación de vulnerabilidades, por complejidad

7.1.4 Vulnerabilidades de sistemas operativos, navegadores y aplicaciones

Comparar las vulnerabilidades de los sistemas operativos con aquellas otras que afectan a otros componentes requiere determinar en primer lugar si tal programa o componente concreto debe ser considerado o no parte del sistema operativo, cosa que no siempre es sencilla[114].

Para facilitar el análisis, podemos distinguir tres diferentes tipos de vulnerabilidades[115]:

- Las **vulnerabilidades del sistema operativo** son aquellas que afectan al núcleo del sistema operativo de que se trate o a sus componentes esenciales.

- Las **vulnerabilidades del navegador** son aquellas que afectan a los componentes de un navegador web, tanto si se distribuye con un sistema operativo concreto[116], como si se trata de software independiente[117].

- Las **vulnerabilidades de las aplicaciones** son aquellas que afectan al resto de los componentes, incluidos los archivos ejecutables, servicios y cualesquiera otros componentes[118].

La figura siguiente muestra la evolución de las vulnerabilidades relativas a los sistemas operativos, navegadores y aplicaciones.

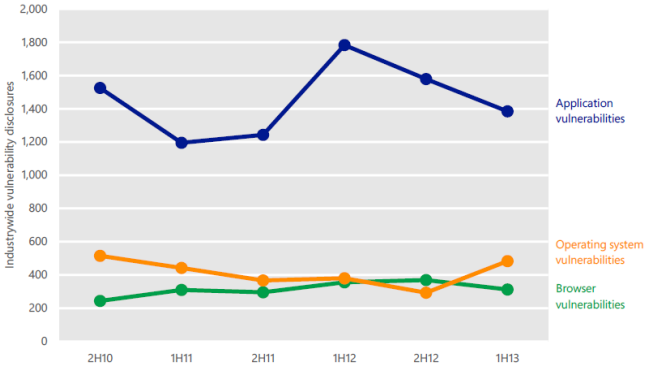
114 Algunos programas (como los reproductores multimedia, por ejemplo) suelen estar preinstalados en el software de sistema operativo (aunque también puedan descargarse de la página web del fabricante). Algunas distribuciones de Linux se ensamblan a partir de componentes desarrollados por diferentes desarrolladores, muchos de los cuales poseen funciones operativas cruciales, tales como interfaces gráficas de usuario (GUI) o los navegadores.

115 Clasificación propuesta por Microsoft.

116 Tales como Internet Explorer (de Microsoft) o Safari (de Apple).

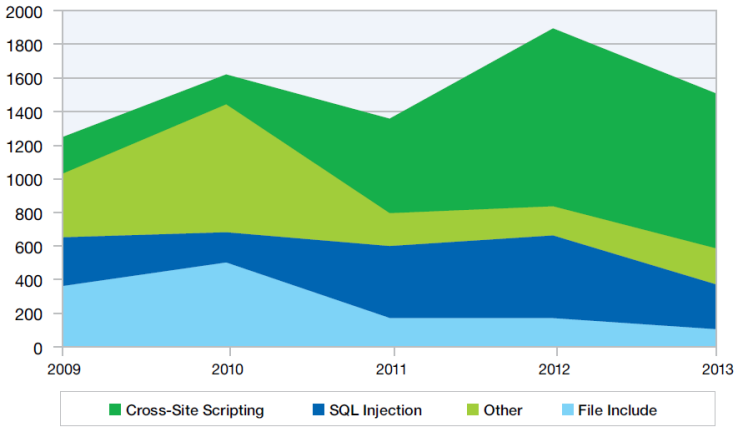
117 Tales como Firefox (Mozilla) o Chrome (Google).

118 Las vulnerabilidades de componentes de código abierto que puedan ser incorporadas a distribuciones de Linux (tales como el sistema de ventanas X , el entorno de escritorio GNOME, el programa de manipulación de imágenes de GNU (GIMP) y otros) se considerarán vulnerabilidades de aplicaciones.



Vulnerabilidades de los sistemas operativos, navegadores y aplicaciones

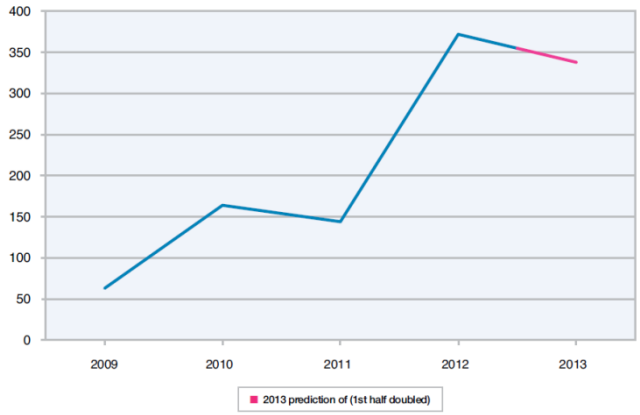
Finalmente, hay que señalar que la mayoría de las vulnerabilidades documentadas se encuentran en los programas de aplicación para web. En el primer semestre de 2013, el 31% de las vulnerabilidades divulgadas fueron aplicaciones utilizadas en servicios Web. Este número se ha reducido significativamente desde 2012, donde se alcanzaron niveles del 42%. Más de la mitad de todas las vulnerabilidades de las aplicaciones web son Cross-Site Scripting (XSS). La figura siguiente muestra tal evolución.



Evolución de las vulnerabilidades en aplicaciones Web, por técnica de ataque

7.1.5 Las vulnerabilidades de los dispositivos móviles

Aunque las vulnerabilidades que afectan a las aplicaciones y a los sistemas operativos de los dispositivos móviles representan un porcentaje relativamente pequeño en comparación con el total de las vulnerabilidades divulgadas (en torno al 4%, en 2013), se ha apreciado un incremento significativo en los últimos años, tal y como muestra la figura siguiente.



Evolución de las vulnerabilidades en dispositivos móviles desde 2009

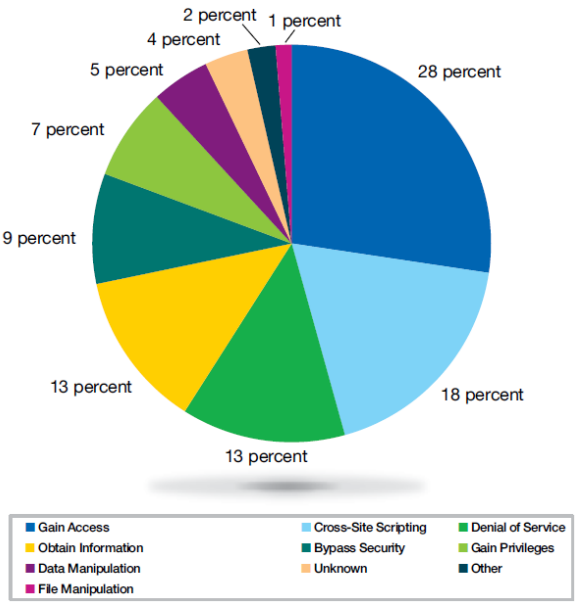
Un aspecto especialmente novedoso tiene que ver con el número de exploits-kits públicos disponibles. En 2013, casi el 30% de todas las vulnerabilidades divulgadas disponía de exploits en comparación con el 9% de las vulnerabilidades divulgadas entre 2009 y 2012.

7.1.6 Las consecuencias de las vulnerabilidades

Las consecuencias (adversas) de las vulnerabilidades en los sistemas de información de las organizaciones pueden ser muy variadas. El cuadro siguiente muestra tales consecuencias, dependiendo del tipo de vulnerabilidad que pueda resultar explotada.

Consequence	Definition
Bypass Security	Circumvent security restrictions such as authentication, firewall, proxy, IDS/IPS system, or virus scanner
Cross-Site Scripting	The impact of cross-site scripting varies depending on the targeted application or victim user, but can include such consequences as sensitive information disclosure, session hijacking, spoofing, site redirection, or website defacement
Data Manipulation	Manipulate data used or stored by the host associated with the service or application
Denial of Service	Crash or disrupt a service or system
File Manipulation	Create, delete, read, modify, or overwrite files
Gain Access	Obtain local and remote access to an application or system. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain access to the underlying service or operating system
Gain Privileges	An attacker using valid credentials can obtain elevated privileges for an application or system
Obtain Information	Obtain information such as file and path names, source code, passwords, or server configuration details
Other	Anything not covered by the other categories
Unknown	The consequence cannot be determined based on insufficient information

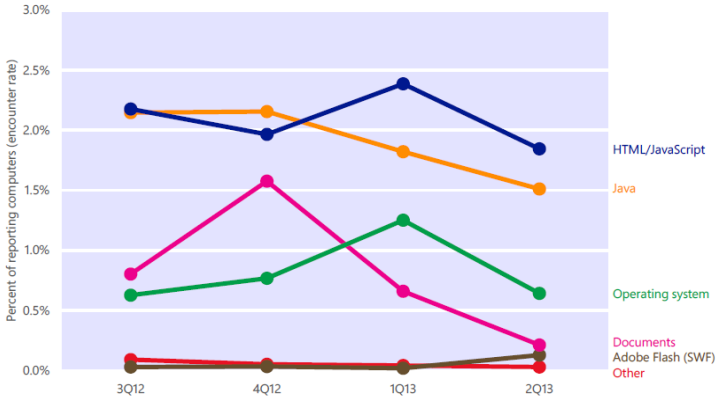
La consecuencia más frecuente de la explotación de una vulnerabilidad en 2013 fue el "acceso", con el 28% de todas las vulnerabilidades reportadas, como se observa en la figura siguiente (para primera mitad de 2013). Este acceso proporciona al atacante el control del sistema afectado, lo que le permite sustraer datos, manipular el sistema, o lanzar otros ataques partiendo de ese sistema. El Cross-Site Scripting contra servicios Web fue la segunda consecuencia más frecuente, con un 18%.



7.2 Exploits

Un exploit es un código dañino que se aprovecha de las vulnerabilidades del software para infectar, interrumpir o tomar el control de un ordenador sin el consentimiento del usuario y, por lo general, sin su conocimiento.

Algunos productos de seguridad pueden detectar y bloquear los intentos de explotar vulnerabilidades conocidas aunque el equipo no esté afectado por éstas. Por ejemplo, la figura siguiente muestra la evolución del empleo de diferentes tipos de vulnerabilidades detectadas por los productos de seguridad de Microsoft.



Ordenadores individuales en los que se detectaron diferentes tipos de intento de explotar vulnerabilidades

7.2.1 Familias de exploits

El cuadro siguiente muestra las familias de exploits más detectadas durante el primer semestre de 2013[119].

Exploit	Platform or technology	3Q12	4Q12	1Q13	2Q13
HTML/IframeRef*	HTML/JavaScript	0.37%	0.58%	0.98%	1.08%
Blacole	HTML/JavaScript	1.60%	1.34%	1.12%	0.62%
CVE-2012-1723	Java	0.84%	1.32%	0.89%	0.61%
CVE-2010-2568 (MS10-046)	Operating system	0.51%	0.57%	0.57%	0.53%
CVE-2012-0507	Java	0.91%	0.53%	0.49%	0.31%
CVE-2013-0422	Java	—	—	0.38%	0.33%
CVE-2011-3402 (MS12-034)	Operating system	—	0.11%	0.62%	0.04%
Pdfjsc	Document	0.77%	1.56%	0.53%	0.12%
CVE-2013-0431	Java	—	—	0.10%	0.32%
CVE-2010-0840	Java	0.31%	0.17%	0.18%	0.21%

Familias de exploits detectadas (en 1H13)

7.2.2 Vulnerabilidades / Exploits de día cero

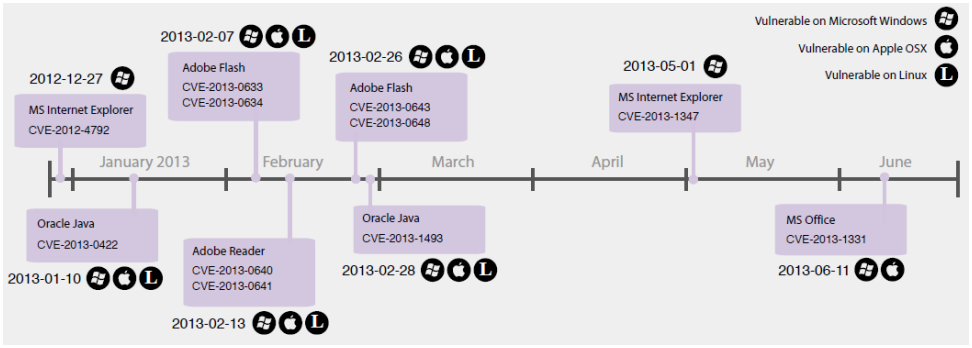
Una vulnerabilidad día cero es un fallo en un software no conocido por su fabricante por lo que no dispone de actualización de seguridad y puede permitir la ejecución de código en el ordenador víctima y su infección. 2013 ha sido un año muy activo en ataques de día cero, especialmente su primer semestre. La mayoría de las acciones de este tipo se localizaron inicialmente en ataques dirigidos.

El año se inició con un ataque de día-cero que explotaba una vulnerabilidad de Internet Explorer (CVE-2012-4792). Los atacantes implantaron el exploit en el sitio web del Council for Foreign Relations. Unos meses después, en mayo de 2013, apareció un exploit para otra vulnerabilidad de día cero (CVE-2013-1347) en Internet Explorer. Similar al primer ataque, el exploit también se encontró en una página web comprometida, esta vez del Department of Labor de los EE.UU.

La figura siguiente muestra la cronología de algunos de los ataques de día cero más significativos, llevados a cabo durante el primer semestre de 2013[120].

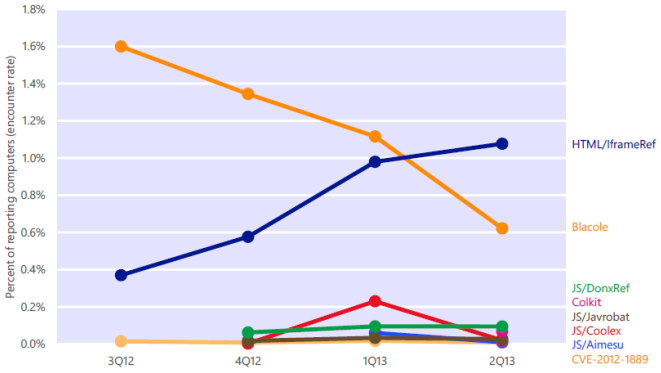
119 Fuente: Microsoft Security Intelligence Report (2013)

120 IBM X-Force: Mid year trend and risk report 2013.



7.2.3 Exploits HTML y JavaScript

La figura siguiente muestra la tasa detección trimestral de los diferentes tipos de exploits HTML y JavaScript durante 2012 y 2013.



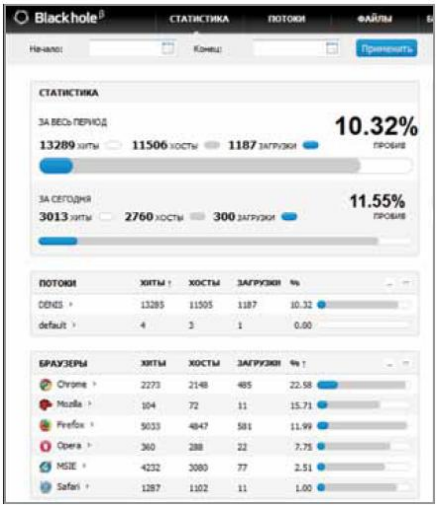
Detección de exploits HTML y JavaScript

7.2.4 Exploits Java

Durante la segunda semana de enero de 2013, se comprobó que dos exploitskits -Blackhole y Cool- estaban atacando vulnerabilidades Java no parcheadas, al objeto de instalar código dañino en los equipos de las víctimas. Algunos autores de código dañino incorporaron estos exploits a sus propios desarrollos[121].

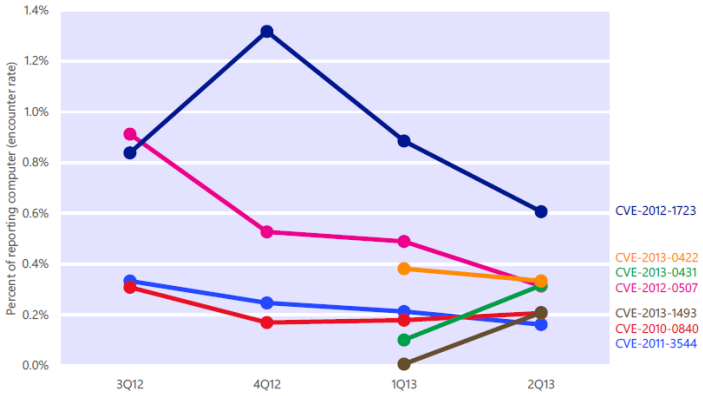
121 http://código dañino.dontneedcoffee.com/2013/01/0-day-17u10-spotted-in-while-disable.html

Por su parte, durante la primera mitad de 2013 Oracle introdujo dos mejoras de seguridad importantes en el funcionamiento de Java. La primera fue la publicación de Java 7u10, que incorporó una función para **desactivar fácilmente Java de un navegador**. El segundo cambio importante se hizo con la publicación de Java 7u11, que cambió el nivel de configuración de seguridad predeterminado, pasándolo a "Alto ", lo que significa que, a partir de ese momento, **se solicita al usuario permiso antes de ejecutar aplicaciones Java sin firmar**.



Panel de Control de BlackHole

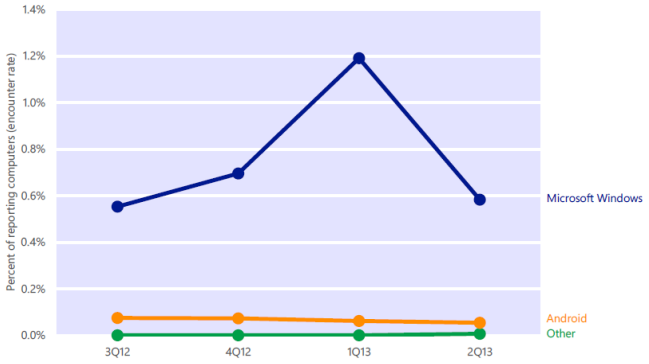
La figura siguiente muestra la tasa de detección de exploits Java en el periodo que se señala.



Detección de exploits Java

7.2.5 Exploits para Sistemas Operativos

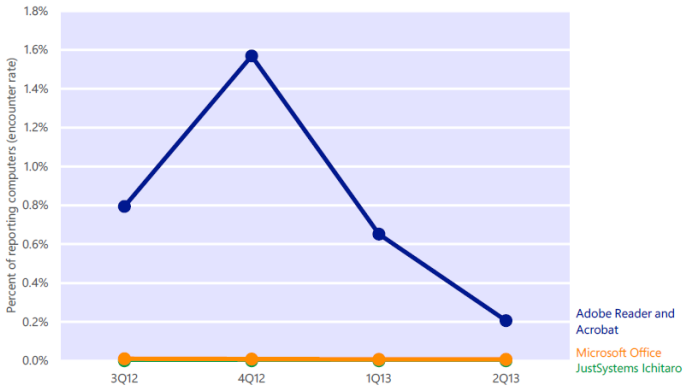
La figura siguiente muestra la tasa de detección de diferentes exploits dirigidos a las vulnerabilidades del sistema operativo.



Detección de exploits contra vulnerabilidades de los sistemas operativos

7.2.6 Exploits para documentos

Los exploits para documentos se dirigen contra vulnerabilidades en los formatos de los documentos o en su visualización o tratamiento. La figura siguiente muestra la detección de este tipo de exploits en el periodo considerado.



Tipos Detección de exploits para documentos detectados

7.2.7 Exploits para Adobe Flash

En febrero de 2013 se explotaron 4 vulnerabilidades de día-cero de Flash Player (CVE-2013-0633, CVE-2013-0634, CVE-2013-0643 y CVE-2013-0648)[122]. Adobe señaló[123] que, desde la introducción de un sandbox para Reader en 2010, el método de entrega más común para los exploits de día-cero de Flash Player había sido a través de documentos de Office. Ya en 2011, en el ataque sufrido por la empresa RSA, os atacantes incrustaron exploits día-cero de Flash en un fichero Excel124.

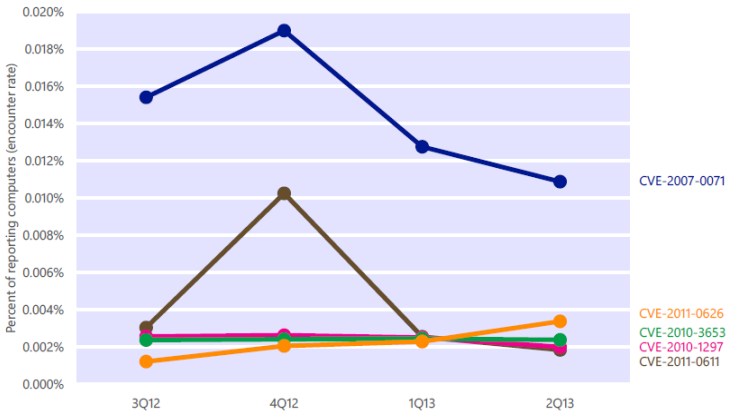
Como decimos, las sofisticadas características de algunos exploits vienen demostrando la capacidad de los atacantes para alcanzar sus objetivos. Desarrollar un exploit capaz de eludir los modernos mecanismos de seguridad –tales como el Address Space Layout Randomization (ASLR), el Data Execution Prevention (DEP) y, en este caso, el sandbox de Reader- y funcionar en una versión actualizada de un sistema operativo, no es tarea fácil y requiere semanas de investigación y desarrollo.

La figura siguiente muestra la detección de diferentes exploits dirigidos contra Adobe Flash Player.

122 http://www.adobe.com/support/security/bulletins/apsb13-04.html

123 http://blogs.adobe.com/asset/2013/02/raising-the-bar-for-attackers-targeting-flash-player-via-office-files.html

124 https://blogs.rsa.com/anatomy-of-an-attack/

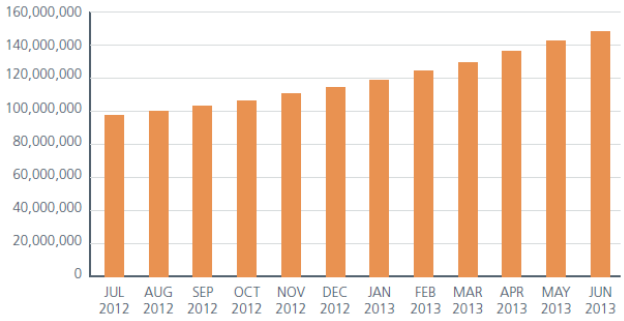


Exploits detectados contra Adobe Flash Player

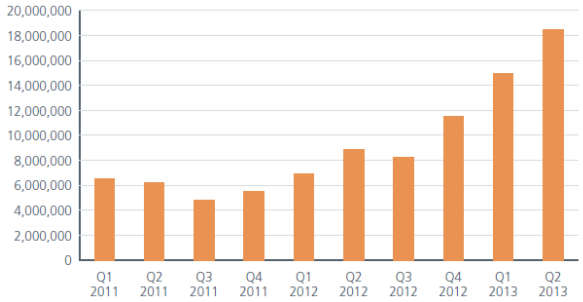
7.3 Código dañino

7.3.1 Crecimiento del código dañino en todo el mundo

El código dañino no da señales de alterar su constante ritmo de crecimiento, que ha aumentado considerablemente durante 2013. Así, a finales del segundo trimestre de 2013 se habían detectado más de 147 millones de muestras de código dañino, tal y como se muestra en la figura siguiente[125].

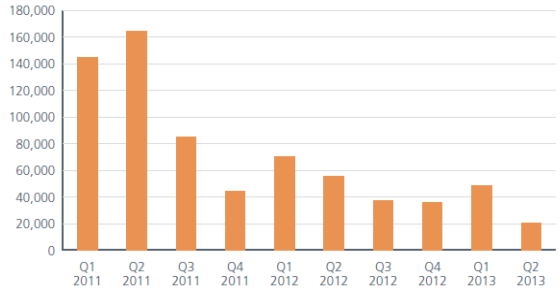


De los que más de 18 millones son muestras nuevas, tal y como se muestra en la figura siguiente.

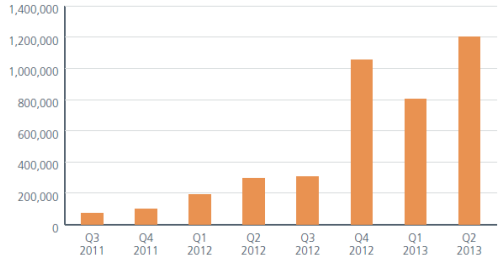


125 Fuente: McAfee Threats Report (SQ, 2013)

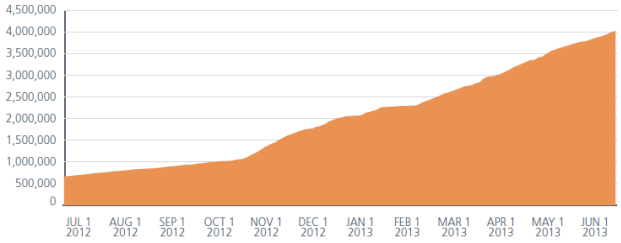
Por otro lado, los rootkits (código dañino oculto), están diseñados para evadir la detección y residir en un sistema por períodos prolongados. El crecimiento de nuevas muestras de rootkits ha tenido una tendencia a la baja desde mediados del 2011. La figura siguiente muestra esta tendencia.



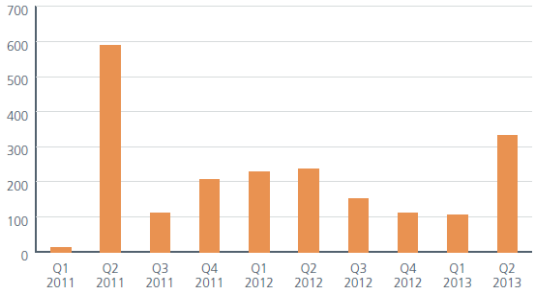
Por su parte, el código dañino firmado se recuperó desde su caída en el primer trimestre de 2013 y otra vez estableció un nuevo récord, con más de 1,2 millones de nuevos ejemplares descubiertos durante el segundo trimestre de 2013, tal y como muestra la figura siguiente.



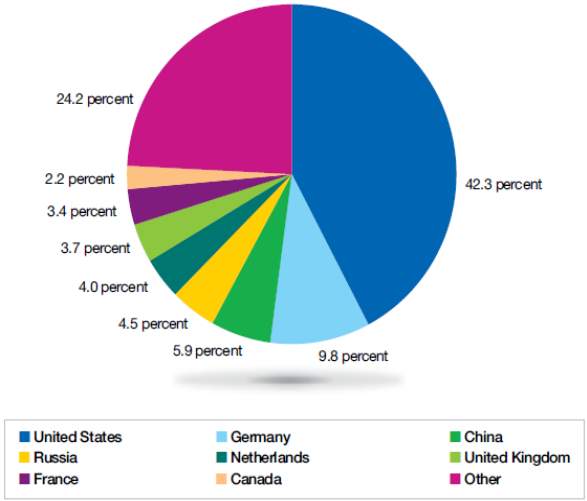
La figura siguiente muestra la tendencia de detección del código dañino firmado nuevo.



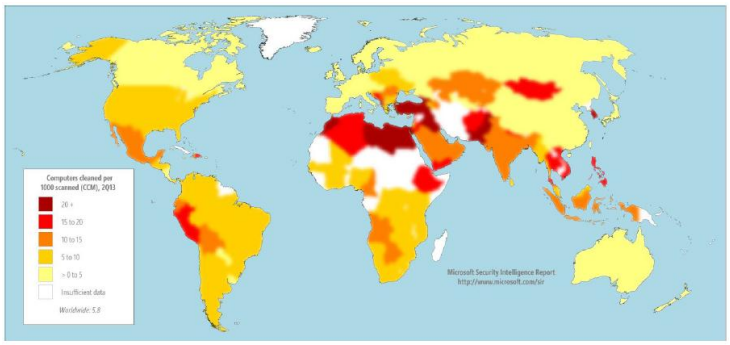
Por su parte, el código dañino nuevo que ataca equipos Mac se ha triplicado, tal y como se muestra en la figura siguiente, después de haber disminuido durante tres trimestres. A pesar de representar cifras menores que el código dañino para PC, es obvio que los usuarios de Mac también necesitan protección.



La figura siguiente muestra los países en los que se alojan los enlaces dañinos y los servidores de Mando y Control (C&C) que sirven exploits. Como se observa, los EE.UU. se encuentran a la cabeza, acogiendo más del 42% de todos los enlaces dañinos. La segunda mayor concentración se encuentra en Alemania, con casi el 10%. Los siguientes cinco países (China, Rusia, Países Bajos, Reino Unido y Francia) tienen cantidades muy similares de enlaces dañinos.

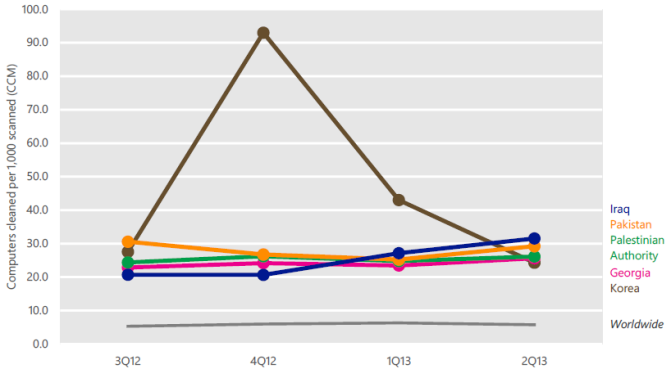


La figura siguiente muestra las tasas de infección mundial en el segundo trimestre de 2013.



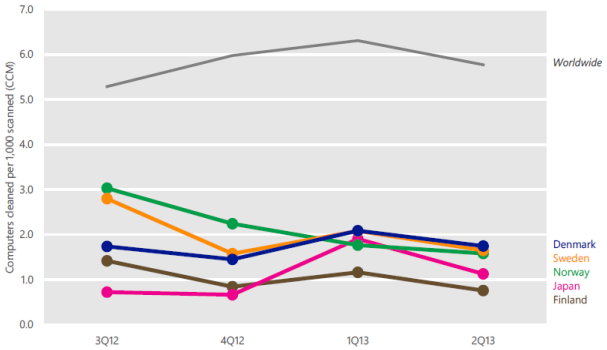
Tasa de infección mundial (2Q13)

Las tasas de infección y de detección por países pueden variar significativamente de un trimestre a otro. En particular, los incrementos en las tasas de detección pueden ser causadas no sólo por el aumento del código dañino en esa ubicación, sino también por un mayor despliegue de las soluciones de seguridad y por mejoras en la capacidad de detección de éstas. La figura siguiente ilustra algunas tendencias de países específicos de todo el mundo que poseen significativas incidencias (Alta o Baja) de infección.



Ubicaciones con la tasa más alta de infecciones por código dañino

La figura siguiente muestra las ubicaciones con la más baja tasa de infección por código dañino.



Ubicaciones con las más bajas tasas de infección por código dañino

En anexo D se presenta información de código dañino del informe Microsoft Security Intelligence Report (2013).

7.3.2 Software de seguridad falso

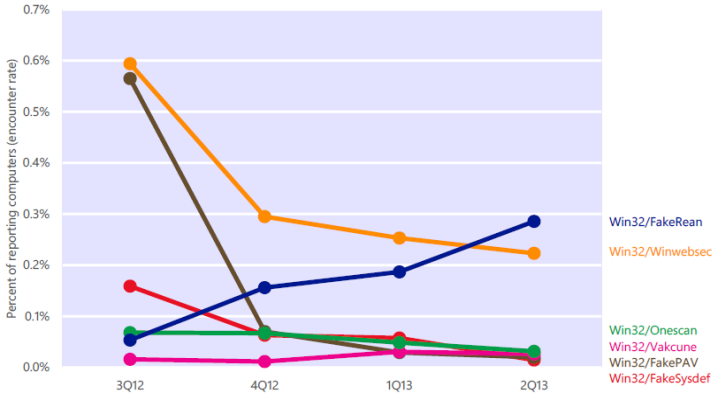
El software de seguridad falso **(scareware)** se ha convertido en uno de los métodos más comunes que usan los atacantes para estafar a las víctimas. Éste pareciendo útil y legítimo, ofrece poca o ninguna seguridad, generando alertas erróneas o engañosas, o desarrollando intentos de atraer a los usuarios a participar en transacciones fraudulentas.

Estos programas suelen imitar el aspecto general y la sensación de programas legítimos de software de seguridad, exhibiendo su potencia para detectar un gran número de amenazas inexistentes al tiempo que instan a los usuarios a pagar por la llamada "versión completa" del software.

Los atacantes suelen instalar programas de software de seguridad falso usando código dañino que aprovecha vulnerabilidades, o utilizando ingeniería social para engañar a los usuarios haciéndoles creer que los programas son legítimos y útiles[126].

Marcas falsas usadas por programas falsos

La figura siguiente muestra la tendencia de detección de las familias de software de seguridad falso más frecuentemente detectadas.



Tendencias de detección de software de seguridad falso

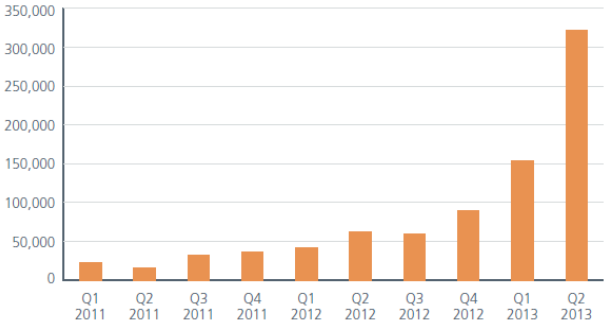
7.3.3 Ransomware

Como es sabido, el *ransomware* es un tipo de código dañino diseñado para hacer que un equipo o sus archivos permanezcan inutilizables hasta que el usuario paga una cierta cantidad de dinero al atacante, a modo de "rescate". Frecuentemente, este software adopta una apariencia oficial o gubernamental, acusando al usuario de la comisión de un delito y exigiendo que el usuario pague una multa a través de transferencia electrónica de dinero si desea recuperar el control del ordenador.

126 Algunas versiones emulan la apariencia del Windows Security Center de Microsoft o, ilegalmente, utilizan marcas o signos distintivos comerciales ampliamente conocidos.

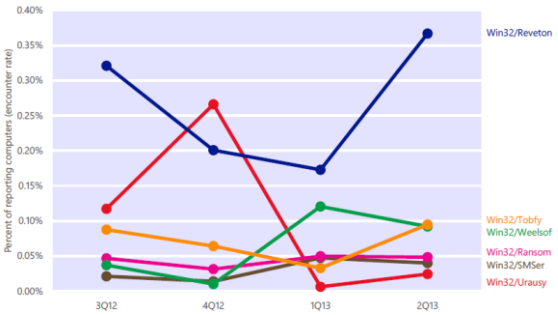
Algunas familias de ransomware operan mostrando una pantalla de bloqueo y evitando el acceso a cualquiera de las funciones del ordenador. Otras, cifran los archivos con una contraseña y ofrecen proporcionar al usuario tal contraseña mediante el pago del correspondiente rescate. Con frecuencia, el acceso al ordenador no se restablece, incluso después del pago.

El número de nuevas muestras aparecidas sólo en el segundo trimestre de 2013 fue superior a 320.000, más del doble que en el trimestre anterior, tal y como se muestra en la figura siguiente.



Una de las razones para el espectacular crecimiento del *ransomware* es que se trata de un medio muy eficaz para los ciberdelincuentes de ganar dinero, toda vez que utilizan los distintos servicios de pago anónimos disponibles. Este método de recolección de dinero es superior a la utilizada por los productos antivirus falsos, por ejemplo, que deben procesar los pedidos hechos mediante tarjetas de crédito. Tales ventajas hacen suponer que el problema del *ransomware* se incrementará en 2014.

La figura siguiente muestra la tasa de detección mundial de las familias de ransomware más usuales.

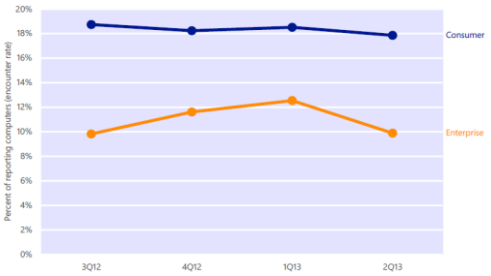


Tasa de detección mundial de ransomware

7.3.4 Código dañino para equipos personales y corporativos

Los patrones de uso de los ordenadores por parte de usuarios privados y usuarios de las organizaciones suelen ser muy diferentes. Los usuarios corporativos usan los equipos para propósitos profesionales, están conectados a una red corporativa, y pueden estar sujetos a limitaciones respecto del uso de Internet y del correo electrónico[127]. Sin embargo, los usuarios domésticos tienen más probabilidades de conectarse a Internet en cualquier momento, directamente o a través de un router doméstico, y usar sus equipos para otros propósitos (principalmente entretenimiento). Como resultado de este diferente comportamiento, los productos de seguridad enfocados a las organizaciones tienden a notificar tasas de detección claramente diferentes de los reportados por los productos de seguridad orientados al consumidor final.

La figura siguiente muestra las tasas de detección de código dañino en los ordenadores de los usuarios domésticos y de los usuarios corporativos en el primer semestre de 2013.



Código dañino detectado en ordenadores domésticos y corporativos

Los resultados arrojados por la figura anterior obedecen a que los entornos corporativos suelen aplicar medidas de defensa en profundidad, tales como firewalls corporativos, lo que dificulta que cierto código dañino pueda llegar a los ordenadores de los usuarios. Por tanto, los ordenadores de las organizaciones tienden a detectar menor número de código dañino que los ordenadores domésticos.

Las figuras siguientes muestran la lista de las 10 principales familias de código dañino detectadas por las organizaciones y los usuarios domésticos, en la primera mitad de 2013.

127 La Guía CCN-STIC 821 muestra una relación de Normas de Seguridad en tal sentido.

	Family	Most significant category	3Q12	4Q12	1Q13	2Q13
1	JS/Seedabutor	Miscellaneous Trojans	—	—	7.3%	2.4%
2	HTML/IframeRef	Exploits	0.6%	5.8%	2.6%	1.9%
3	Win32/Conficker	Worms	2.3%	2.1%	1.8%	1.4%
4	INF/Autorun	Miscellaneous Trojans	1.8%	1.8%	1.6%	1.4%
5	Win32/Sirefef	Miscellaneous Trojans	1.0%	0.8%	1.5%	1.2%
6	JS/BlacoleRef	Miscellaneous Trojans	1.5%	1.1%	1.2%	1.3%
7	Java/CVE-2012-1723	Exploits	1.1%	1.7%	1.3%	0.9%
8	Blacole	Exploits	1.3%	1.4%	1.5%	0.7%
9	Win32/Dorkbot	Worms	0.8%	0.8%	0.7%	0.7%
10	Win32/Obfuscator	Miscellaneous Trojans	0.7%	0.6%	0.6%	0.6%

Código dañino más frecuentemente detectado en equipos corporativos[128]

	Family	Most significant category	3Q12	4Q12	1Q13	2Q13
1	INF/Autorun	Miscellaneous Trojans	4.1%	3.9%	3.3%	3.4%
2	Win32/Obfuscator	Miscellaneous Trojans	2.2%	2.4%	2.6%	3.8%
3	HTML/IframeRef	Exploits	0.8%	3.4%	2.7%	3.3%
4	JS/Seedabutor	Miscellaneous Trojans	—	—	3.0%	1.3%
5	Win32/Dorkbot	Worms	1.8%	1.9%	1.5%	1.9%
6	Win32/Sirefef	Miscellaneous Trojans	2.0%	1.4%	1.6%	1.4%
7	Win32/Sality	Viruses	1.5%	1.6%	1.4%	1.5%
8	Win32/Gamarue	Worms	0.2%	0.2%	0.6%	2.1%
9	Win32/Conficker	Worms	1.6%	1.5%	1.3%	1.3%
10	JS/BlacoleRef	Miscellaneous Trojans	1.7%	1.1%	0.8%	1.5%

Código dañino más frecuentemente detectado en equipos domésticos

7.4 Sofware Potencialmente No Deseado

Se entiende por Software Potencialmente No Deseado a aquellos programas que, pese a representar un riesgo de seguridad moderado o bajo, pueden afectar a la privacidad, la seguridad o la experiencia informática de los usuarios. La figura siguiente muestra los diez países del mundo con la mayor tasa de detección de este tipo de software, durante la primera mitad de 2013.

	Country/Region	3Q12	4Q12	1Q13	2Q13	Chg. 2H–1H
1	United States	7.42%	4.29%	4.99%	3.79%	-25.04% ▼
2	Brazil	15.73%	23.58%	23.04%	16.31%	0.09% ▲
3	Russia	17.52%	14.43%	15.41%	11.58%	-15.53% ▼
4	Turkey	32.90%	16.44%	16.11%	12.23%	-42.55% ▼
5	India	16.73%	12.34%	11.59%	9.28%	-28.21% ▼
6	Mexico	13.11%	12.82%	13.21%	10.07%	-10.24% ▼
7	Germany	7.68%	5.44%	6.74%	3.55%	-21.56% ▼
8	France	10.34%	10.03%	12.37%	6.38%	-7.92% ▼
9	China	6.37%	4.56%	4.03%	3.47%	-31.39% ▼
10	United Kingdom	8.24%	6.07%	7.40%	4.97%	-13.53% ▼

Países con la mayor tasa de detección de software potencialmente no deseado (1H13)

128 Usando los productos de seguridad corporativa de Microsoft.

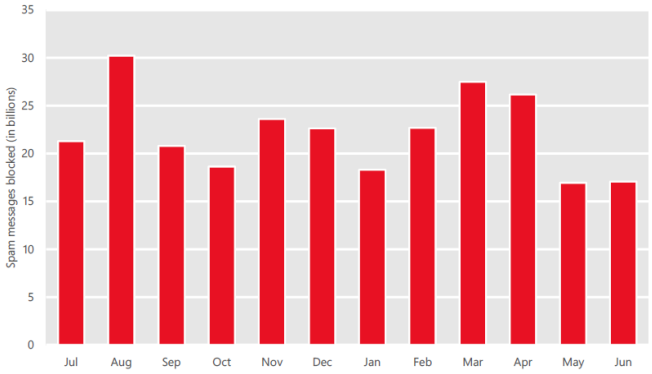
7.5 Amenazas contra el correo electrónico

Según Microsoft[129], más del 75% de los mensajes de correo electrónico enviados a través de Internet son no deseados. Esto no sólo contribuye a congestionar las bandejas de entrada y a dificultar la gestión de recursos, sino que, también, crea un entorno que facilita la remisión de código dañino y phishing. Los proveedores de correo electrónico, las redes sociales y otras comunidades online han hecho del bloqueo del spam, del phishing y de otras amenazas del correo electrónico, una prioridad absoluta.

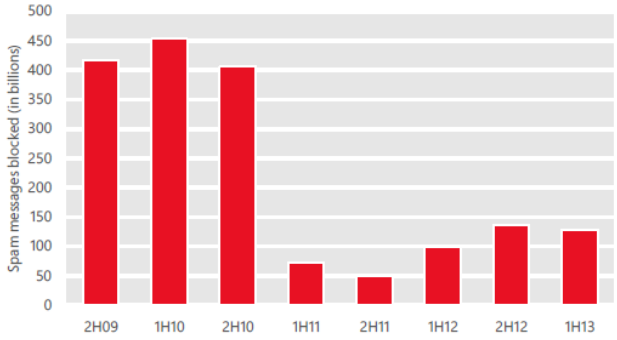
La información de esta sección es una compilación de los datos de telemetría proporcionados por Exchange Online Protection de Microsoft, que proporciona datos sobre spam, phishing y filtrado de código dañino.

7.5.1 Correo no deseado (spam)

La figura siguiente muestra los mensajes de spam bloqueados en el periodo junio 2012 – junio 2013.



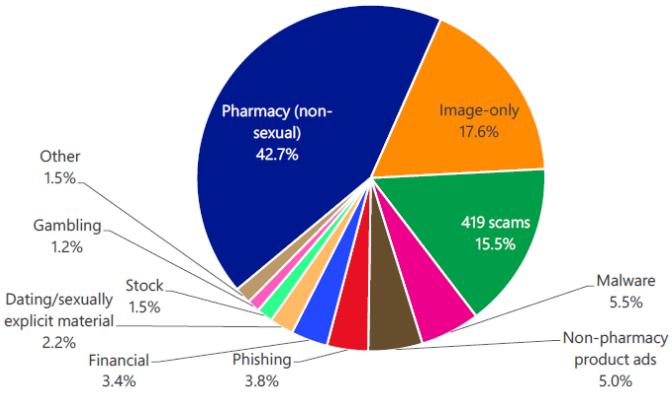
La figura siguiente muestra los mensajes bloqueados semestralmente desde la segunda mitad de 2009. Se muestra una clara tendencia a la baja en el correo no deseado.



129 Vol. 15 - Microsoft Security Intelligence Report (2013)

7.5.2 Tipos de spam

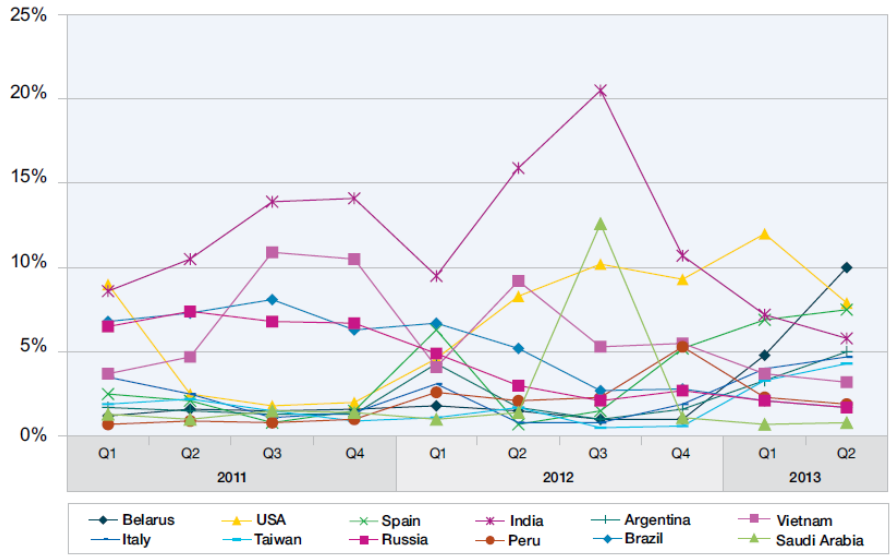
Algunos filtros[130] reconocen varios de los tipos más comunes de mensajes de spam. La figura siguiente muestra la prevalencia relativa de los tipos de spam que se detectaron en la primera mitad de 2013.



7.5.3 Orígenes geográficos de las botnet para spam

Para evaluar el impacto que tienen las botnets en el spam, pueden monitorizarse los mensajes de spam enviados desde direcciones IP que hubieren sido asociados con botnets conocidas, realizando búsquedas geográficas en las direcciones IP de origen. Identificar desde dónde envía el spam la botnet resulta de utilidad para los CERT de cara a valorar la magnitud de los problemas de seguridad que afectan a diferentes áreas geográficas.

La figura siguiente muestra las localizaciones de origen del spam, desde 2011 hasta el segundo trimestre de 2013.

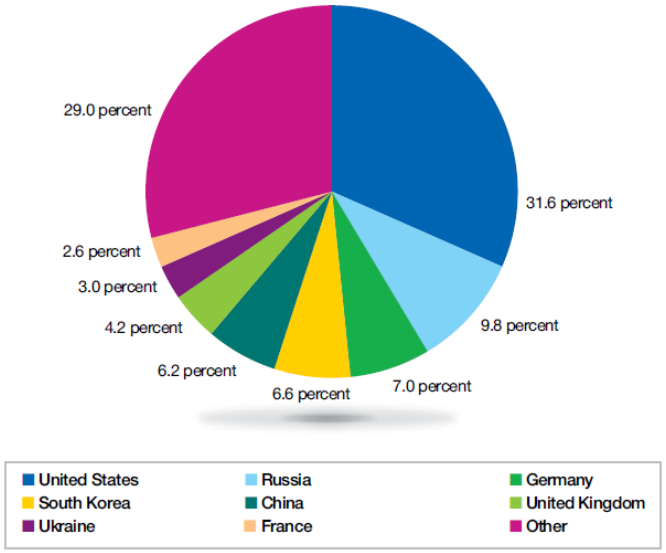


130 Tales como el Exchange Online Protection, de Microsoft, del que están tomados los siguientes datos estadísticos.

De la figura anterior se pueden extraer algunas conclusiones:

- **Bielorrusia** tiene una presencia muy fuerte, remitiendo el 10% del spam detectado.
- En el primer trimestre de 2013, y por primera vez en dos años, los EE.UU. lideraron el ranking, con el envío de un 12%, disminuyendo al 8% en el segundo trimestre.
- En el **primer semestre de 2013, España se situó dentro de los tres primeros lugares**, por primera vez en años.
- Si bien la India dominaba la escena a finales de 2012, enviando más de una quinta parte de todo el spam mundial, en 2013 fue superada por Bielorrusia, EE.UU. y España.
- Argentina e Italia llegaron a los cinco y seis primeros lugares, respectivamente, por primera vez en años.
- Arabia Saudita no repitió su actuación del tercer trimestre de 2012 y se mantiene estable en torno al 1%.

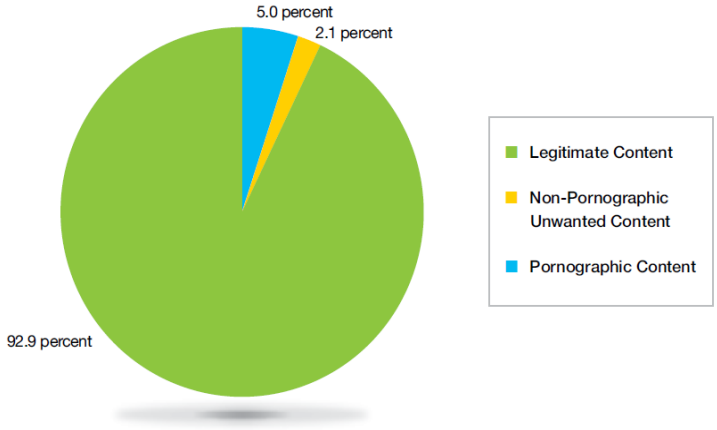
La figura siguiente muestra aquellos países donde se ha detectado el mayor alojamiento de Servidores C&C de botnets.



7.6 Sitios web dañinos

Frecuentemente, los agentes de las amenazas utilizan sitios web para iniciar ataques de phishing o distribuir código dañino. Los sitios web dañinos tienen generalmente un aspecto totalmente legítimo, incluso para usuarios experimentados. En muchos casos, tales sitios son páginas web legítimas que han sido previamente comprometidas por el atacante, en un intento de aprovecharse de la confianza que tienen tales sitios. Para ayudar a proteger a los usuarios de las páginas web maliciosas, los fabricantes de navegadores han desarrollado filtros que hacen un seguimiento de los sitios que almacenan código dañino o han desarrollado ataques de phishing, mostrando advertencias cuando el usuario intenta navegar en ellas.

Los resultados obtenidos por un reciente estudio[131], señalan que cerca del 93% de los sitios web analizados contienen contenidos legítimos. Sólo un 5% albergan contenidos pornográficos o contenidos expresamente no deseados (2,1%). La figura siguiente muestra estos porcentajes.

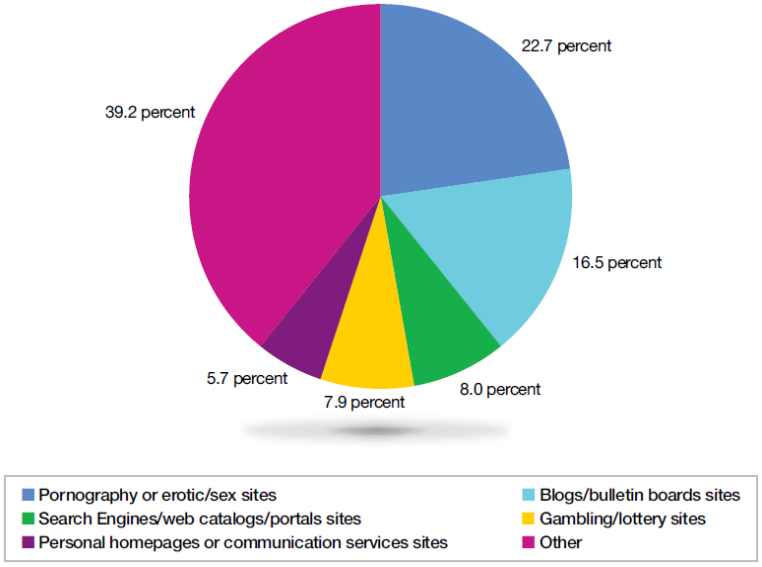


Algunas consecuencias del estudio anterior son las siguientes:

- El área de contenidos con **mayor nivel de riesgo** se encuentra en los **sitios de pornografía**. Estos sitios fueron responsables de casi el 23% de todos los enlaces dañinos detectados.
- Los **sitios web dinámicos –blogs–**, donde los usuarios pueden aportar contenidos a través de artículos, comentarios y mensajes, constituyen la segunda área más peligrosa de la Internet (16,5%).
- Algunos sitios, tradicionalmente reputados como "seguros", alojan un significativo porcentaje (entre el 5,7 y el 8%) de enlaces o contenidos dañinos.
- Los sitios de juego, que alojan el 7,9% de todos los enlaces dañinos.
- El 39% restante se encuentran ampliamente distribuidos en otras categorías.

La figura siguiente muestra esta distribución.

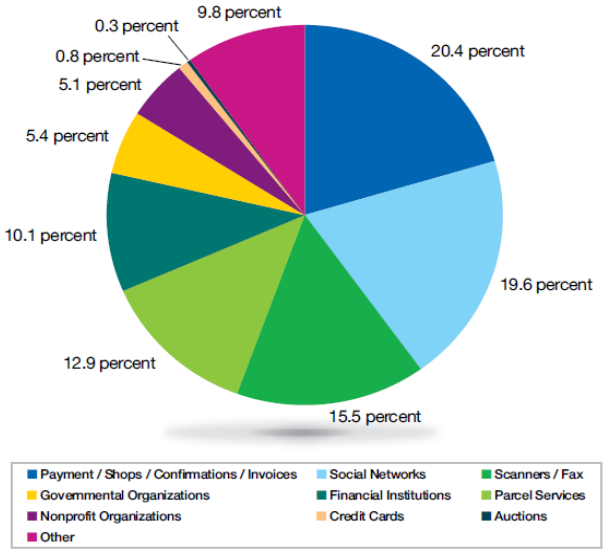
131 Con datos obtenidos de Alexa (http://www.alexa.com/), una de las empresas más conocidas de información de la WWW.



7.6.1 Organizaciones objetivo de las estafas y el phishing

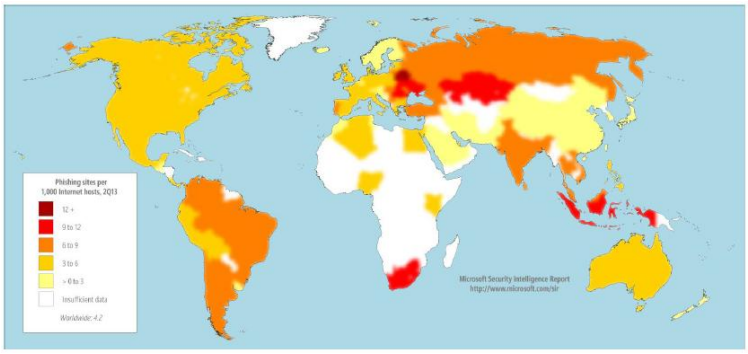
La figura siguiente muestra los objetivos de las estafas y del phishing en la primera mitad de 2013. Los datos se han calculado en base a las siguientes consideraciones:

- Las estadísticas se basan exclusivamente en campañas de estafas/phishing desplegadas a través del correo electrónico.
- Las estadísticas incluyen todos los correos electrónicos que mencionan nombres de confianza o marcas conocidas, al objeto de que los usuarios descarguen un archivo adjunto.



7.6.2 Distribución mundial de sitios de phishing

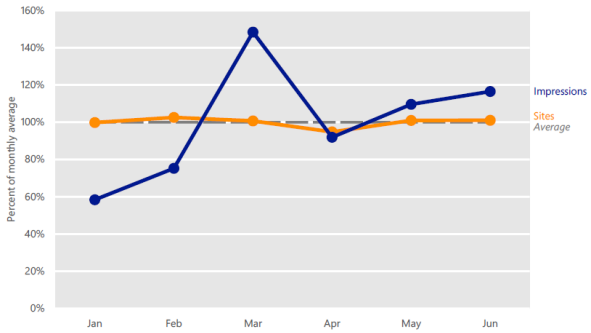
Los sitios de phishing suelen alojarse en hosts de alojamiento gratuito o en servidores web comprometidos. La figura siguiente muestra la ubicación de los sitios phishing, por cada 1.000 hosts de Internet, en el segundo trimestre de 2013.



7.6.3 Los sitios de alojamiento de código dañino

Ciertos filtros antispam y anticódigo dañino ayudan a proporcionar protección contra los sitios conocidos por alojar código dañino o sitios de phishing. Algunos de ellos utilizan datos reputacionales de direcciones URL, así como mecanismos específicos para determinar si los sitios distribuyen contenido no seguro.

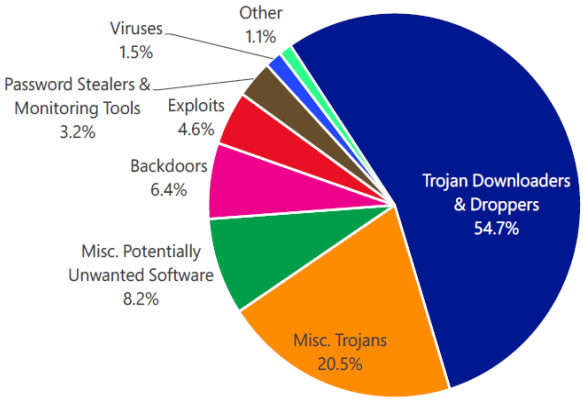
La figura siguiente compara mensualmente la cantidad de hosts de código dañino activos con el volumen de evidencias de código dañino detectadas[132].



7.6.4 Categorías de código dañino

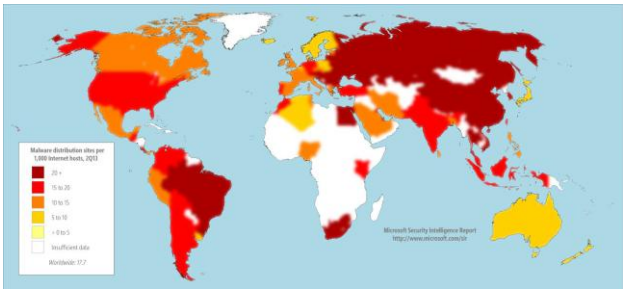
La figura siguiente muestra los tipos de amenazas alojadas en las URL que fueron bloqueadas por el filtro SmartScreen en el primer trimestre de 2013.

132 Datos obtenidos usando SmartScreen Filter, Internet Explorer y la base de datos de código dañino de Microsoft.



7.6.5 Distribución de los sitios de alojamiento de código dañino

La figura siguiente muestra la distribución geográfica de los sitios de alojamiento de código dañino reportados.



Consideraciones:

- Los sitios que alojaron código dañino fueron significativamente más frecuentes que los sitios de phishing en la primera mitad de 2013. Así, se detectaron 11,7 sitios de alojamiento de código dañino por cada 1.000 hosts de Internet en todo el mundo.

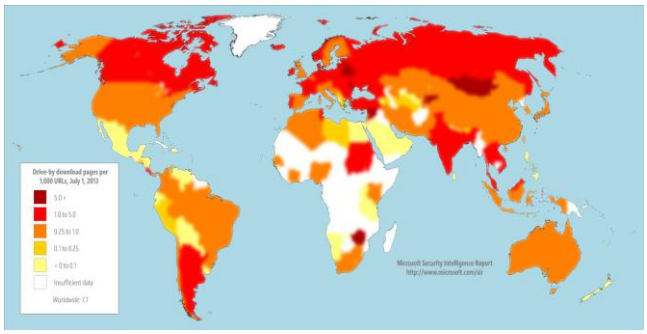
- China, que tenía una concentración inferior a la media de sitios de phishing (2,3 sitios por cada 1.000 servidores de Internet en el segundo trimestre de 2013), también tuvo una muy alta concentración de sitios de alojamiento de código dañino (37,7 sitios por cada 1.000 anfitriones). Otros lugares con gran concentración de sitios de alojamiento de código dañino fueron: Ucrania (71,2), Rusia (43,6) y Brasil (33,6). Los lugares con menores concentraciones de sitios de alojamiento de código dañino fueron: Finlandia (6,1), Dinamarca (7,0) y Japón (7,0).

7.6.6 Sitios de descarga Drive-by

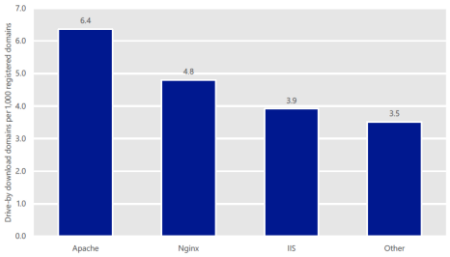
Un sitio de descarga drive-by es un sitio web que aloja uno o varios exploits que atacan las vulnerabilidades de los navegadores web y sus complementos. Así, los usuarios con equipos vulnerables pueden infectarse con código dañino simplemente visitando un sitio web, incluso sin tratar de descargar nada.

Ciertos motores de búsqueda[133] han tomado una serie de medidas para ayudar a proteger a los usuarios de las descargas drive-by. Tales buscadores analizan los sitios web de exploits referenciados y muestran mensajes de advertencia cuando en los resultados de las búsquedas aparecen tales direcciones.

La figura siguiente muestra la concentración de páginas de descarga drive-by de los países y regiones de todo el mundo al final del segundo trimestre de 2013.



Algunas plataformas de software de servidores web tienen más probabilidades de albergar sitios de descarga drive-by que otros debido a una serie de factores, tales como la prevalencia de los exploits kits dirigidos contra plataformas específicas. La figura siguiente muestra la prevalencia relativa de los sitios de descarga drive-by en las diferentes plataformas de servidor web.

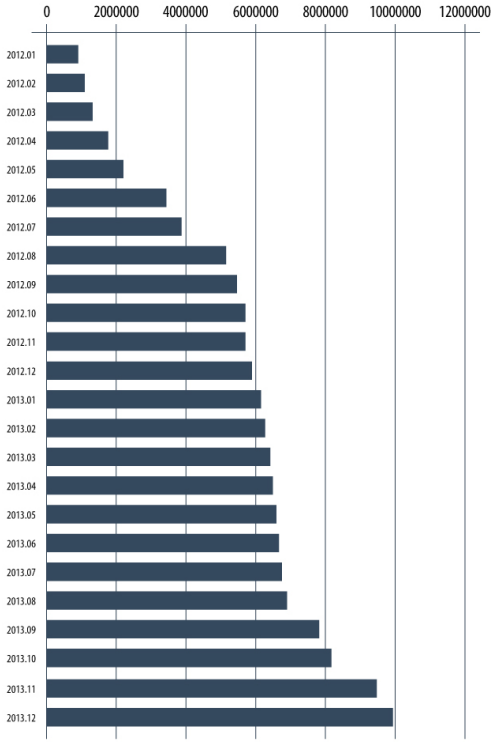


7.7 Amenazas a dispositivos móviles

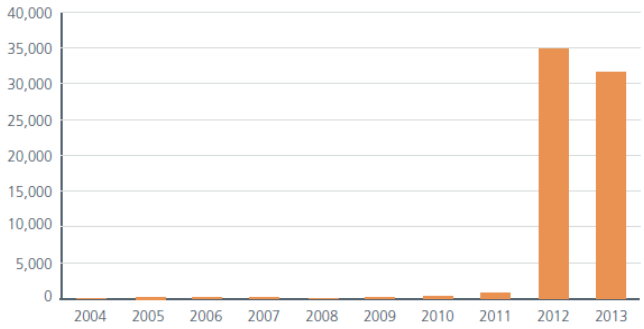
Durante 2013, se ha detectado un total de 143.211 modificaciones nuevas de código dañino para dispositivos móviles. Por otro lado, en 2013, los atacantes usaron 3.905.502 paquetes para la distribución de código dañino. La figura siguiente muestra esta evolución[134].

133 Como Bing, por ejemplo.

134 Fuente: securelist



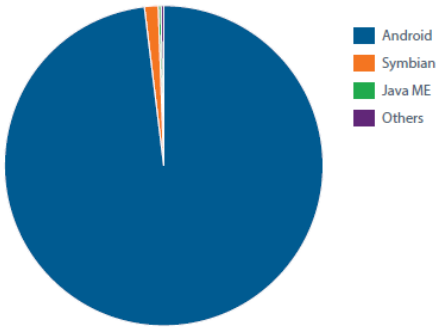
El incremento de código dañino para dispositivos móviles fue enorme durante 2013. Un dato: la empresa McAfee recogió a mediados de 2013 casi tantas muestras de código dañino móvil como en todo el año 2012[135].



Código dañino móvil nuevo (en la primera mitad de 2013)

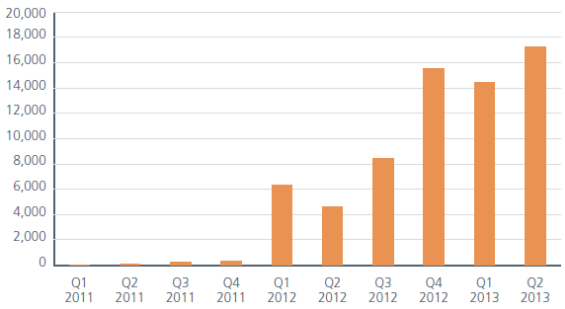
La figura siguiente muestra la distribución de código dañino por sistema operativo móvil.

135 McAfee Threats Report (SQ 2013)



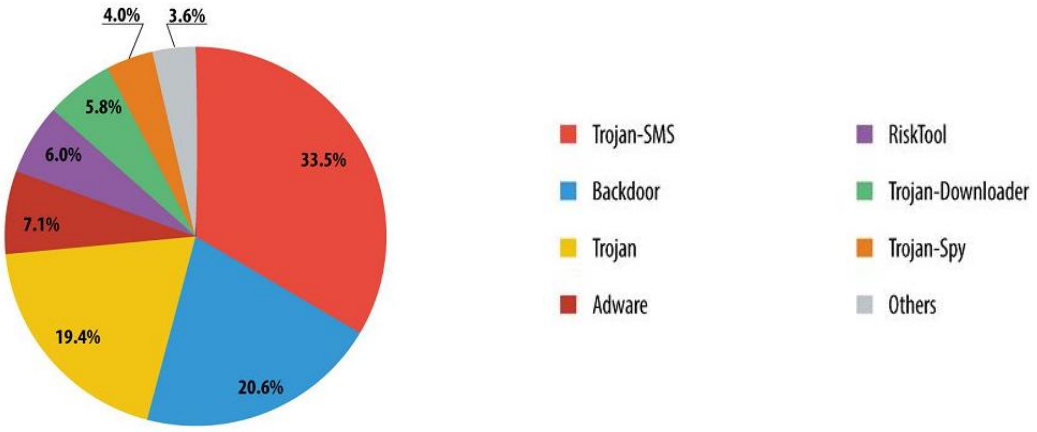
Código dañino Móvil por plataforma (1H13)

En concreto, la figura siguiente muestra la detección de código dañino Android nuevo, por trimestres, desde 2011.



Código dañino Android nuevo (1H13)

La figura siguiente muestra la distribución de código dañino para dispositivos móviles, por categoría.



Finalmente, el cuadro siguiente muestra las 10 amenazas para dispositivos móviles más detectadas en 2013.

	Name*	% of all attacks
1	DangerousObject.Multi.Generic	40.42%
2	Trojan-SMS.AndroidOS.OpFake.bo	21.77%
3	AdWare.AndroidOS.Ganlet.a	12.40%
4	Trojan-SMS.AndroidOS.FakeInst.a	10.37%
5	RiskTool.AndroidOS.SMSreg.cw	8.80%
6	Trojan-SMS.AndroidOS.Agent.u	8.03%
7	Trojan-SMS.AndroidOS.OpFake.a	5.49%
8	Trojan.AndroidOS.Plangton.a	5.37%
9	Trojan.AndroidOS.MTK.a	4.25%
10	AdWare.AndroidOS.Hamob.a	3.39%

7.7.1 Código dañino financiero

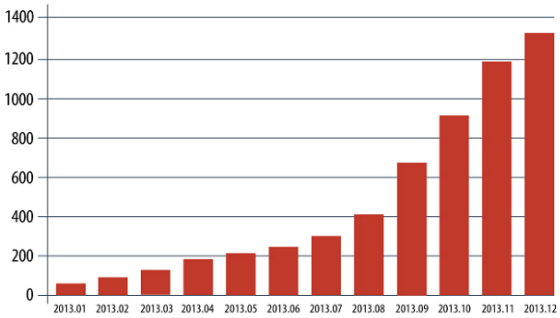
Viene siendo habitual que las entidades financieras de Europa y Asia utilicen autenticación de dos factores a través de mensajes SMS. Cuando los clientes inician sesión se les envía un número de autenticación de transacciones móviles (mTAN) en un mensaje de texto, que el usuario debe introducir para obtener acceso a su cuenta. Este paso evita que un atacante que disponga fraudulentamente del nombre de usuario y la contraseña pueda acceder a la cuenta de la víctima.

Por este motivo, los ciberdelincuentes que pretenden superar la autenticación de dos factores necesitan acceder al mensaje SMS remitido por el banco. Una vez que el atacante ha robado el nombre de usuario y la contraseña desde el PC de la víctima, el ciberdelincuente sólo necesita conseguir que el usuario instale un código dañino que le reenvíe el antedicho SMS. Un ejemplo de estos ataques son las muestras Android/FakeBankDropper.A y Android/FakeBank.A. La primera sustituye la aplicación oficial del banco y la segunda obtiene el última SMS remitida desde el banco[136].

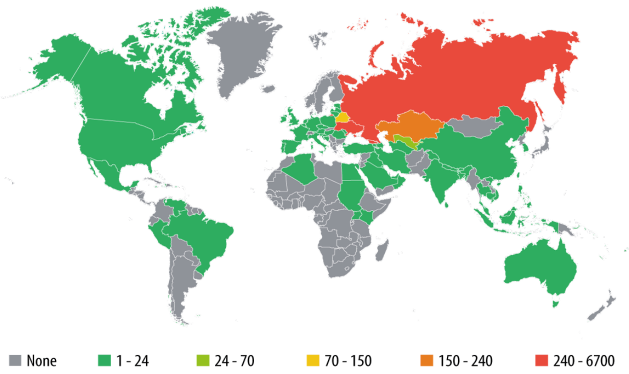
La figura siguiente muestra la evolución del número de troyanos bancarios detectados en 2013.

136 Una breve lista de programas SMS-forward similares:

- Android/Nopoc.A: Reenvía mensajes SMS entrantes al servidor del atacante.
- Android/Pincer.A: Pretende instalar un certificado en el dispositivo del usuario. Reenviando los mensajes SMS al servidor del atacante.
- Android/Stels.A: Se hace pasar por una actualización de Adobe Flash Player. Recopila información confidencial del usuario y la remite al servidor del atacante.
- Android/Wahom.A: Se hace pasar por una aplicación legítima, pero muestra un mensaje de error al usuario. El programa dañino oculta su icono para engañar al usuario haciéndole creer que se ha desinstalado. Recopila información confidencial del usuario y envía SMS al servidor del atacante.



Por su parte, la figura siguiente muestra la distribución mundial de las infecciones causadas por código dañino malicioso para aplicaciones bancarias.



7.7.2 Sólo para adultos

El software de entretenimiento para adultos representa un magnífico camuflaje para los atacantes, que pueden obtener importantes beneficios, siendo además donde la intervención de los cuerpos policiales es menor. Por estos motivos, el interés por este tipo de aplicaciones para adultos se ha incrementado significativamente en 2013.

En Japón, la familia de programas potencialmente no deseados Android/DeaiFraud, se hace pasar por la aplicación de un sitio web para citas muy conocida. Aunque este código dañino no es directamente perjudicial para los usuarios, sin embargo puede ser generador de spam.

Aparte del software anterior, en 2013 se detectó también Android/NMPHost.A, un código dañino que convence a los usuarios para descargar un segundo código dañino, Android/NMP.A, que sustrae información del usuario. Ambos códigos dañinos se hacen pasar por aplicaciones de entretenimiento para adultos.

7.7.3 Troyanos dirigidos

Los atacantes también suelen utilizar aplicaciones legítimas para ocultar código dañino, amparados en la popularidad y la confianza que tiene una determinada aplicación entre sus usuarios. En el caso de Android/Kaospy.A, los atacantes utilizaron versiones modificadas de la aplicación Kakao y pusieron el foco de los ataques en activistas tibetanos. Este código dañino

se distribuye mediante correos electrónicos de phishing. El spyware dañino recopila una gran cantidad de información del usuario (contactos, registros de llamadas, mensajes SMS, aplicaciones instaladas y ubicación) y remite los datos al servidor del atacante.

Algunas aplicaciones infectadas incluyen el código dañino Android/BadNews.A. Este troyano se hace pasar por una aplicación legítima de juego que incluye anuncios. En su lugar, recopila información del usuario y la remite al atacante. También puede mostrar titulares de noticias falsas.

7.7.4 Spyware móvil

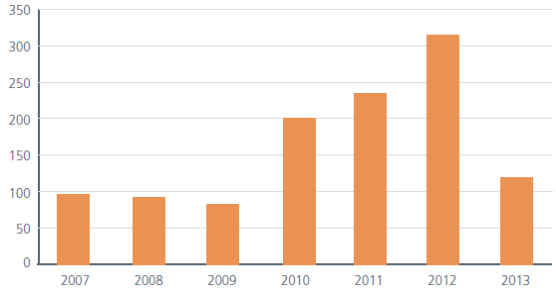
En 2013 el spyware comercial ha aumentado respecto de años anteriores. Así, Android/Fzw.A descarga una aplicación spyware desde el sitio web del atacante. Al igual que otros troyanos ocultos, se hace pasar por un instalador de aplicaciones legítimas. El spyware descargado envía mensajes SMS, registros de llamadas y la información de localización al servidor del atacante.

Por su parte, Android/Roidsec.A es un software espía que se hace pasar por una aplicación para sincronizar el teléfono del usuario. Sin embargo, lo que hace realmente es remitir información y SMS del usuario al servidor del atacante. Este código dañino recoge la ubicación, registros de llamadas y datos sobre el hardware del teléfono, pudiendo además, grabar las llamadas.

7.8 Amenazas a bases de datos

El segundo trimestre de 2013 evidenció una cierta desaceleración en las violaciones de seguridad contra Bases de Datos[137].

La figura siguiente muestra esta tendencia[138].



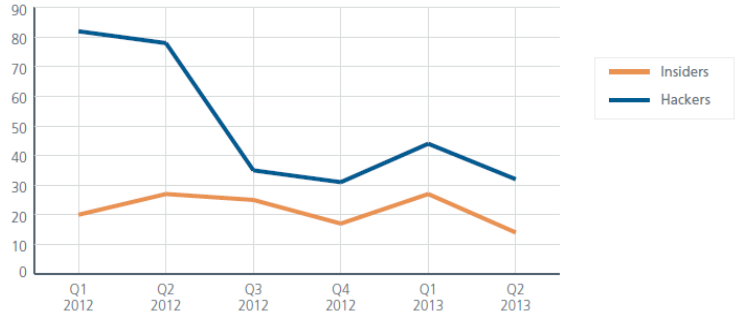
El índice de las violaciones de datos causada por hackers externos (ciberdelincuentes o no) se redujo considerablemente en 2012, y se ha mantenido relativamente estable durante 2013, tal y como se muestra en la figura siguiente[139]. La menor tasa de robo por parte de empleados de las propias organizaciones también se ha mantenido relativamente estable.

137 Obviamente, se trata de aquellas violaciones que se han hecho públicas.

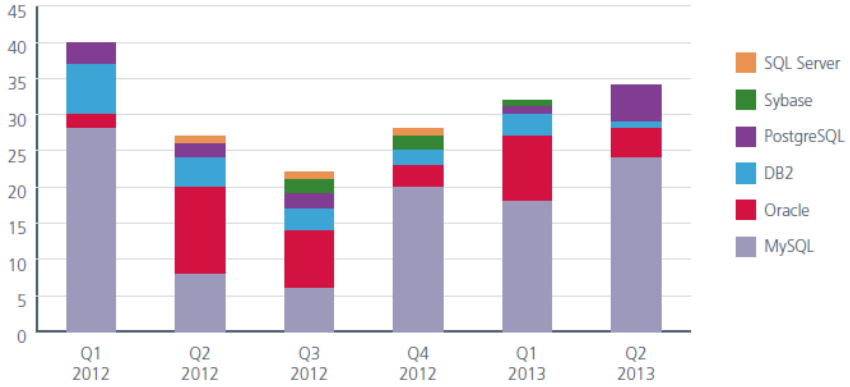
138 Fuente: privacyrights.org

139 Fuente: pricacyrights.org

Parece que la seguridad de las bases de datos recibe más atención por parte de las organizaciones que uno o dos años atrás.



Las vulnerabilidades de las bases de datos reportadas, siguen estando dominadas por MySQL, con casi el 60% de todas las descubiertas en los últimos seis trimestres, tal y como muestra la figura siguiente.



8. LA CIBERSEGURIDAD EN EUROPA

8.1 Panorama de las ciberamenazas en Europa

Atendiendo a lo señalado por ENISA[140], la ciberseguridad europea en 2013 ha estado marcada por las siguientes realidades:

- Los **agentes de las amenazas** han aumentado la sofisticación de sus ataques y sus herramientas.
- La madurez para actuar en el ciberespacio en forma de **ciberespionaje** no es una cuestión de unos pocos Estados-nación. Por el contrario, muchos de estos han desarrollado capacidades que se podrían utilizar para infiltrarse en todo tipo de objetivos, tanto públicos como privados. Los ataques han crecido en intensidad, sofisticación y peligrosidad
- Las **ciberamenazas** han alcanzado a los **dispositivos móviles**: Los patrones de ataque y las herramientas que hasta hace unos años tenían como objetivo a los PCs han migrado al ecosistema de dispositivos móviles.
- Dos nuevas focos de atención: **Big Data** e Internet de las Cosas (***Internet of Things***).
- Los cuerpos policiales han cosechado importantes éxitos: detención del autor del Virus de la Policía, desmantelamiento y clausura de Silk Road, detención del autor de Blackhole, entre otros.
- Los **fabricantes de software** han aumentado la velocidad de respuesta a sus vulnerabilidades.
- Se ha incrementado la cooperación entre las organizaciones competentes en materia de ciberseguridad.
- Se ha iniciado el debate en torno a la legitimidad de la vigilancia relacionada por los Estados.

La figura siguiente muestra una panorámica de las 15 ciberamenazas más significativas, y sus tendencias evolutivas.

140 ENISA Threat Landscape 2013.

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Critical Infrastr.	Mobile Computing	Social Networ-king	Cloud Compu-ting	Trust Infrastr.	Big Data	Internet of Things
1. Drive-by Downloads	↑	↑	↑	↑		↑	↑	
2. Worms/ Trojans	↑	↑	↑	↑	↑	↑	↑	↑
3. Code Injection	↑	↑	↑	→	↑	↑	↑	
4. Exploit Kits	↑	→	↑	↑	↑	↑	↑	
5. Botnets	→	↑	↑	↑	↑			
6. Physical Damage/Theft /Loss	↑	↑	↑	↑	↑	↑	↑	↑
7. Identity Theft/Fraud	↑		↑	↑	↑	↑	↑	↑
8. Denial of Service	↑	↑			↑			↑
9. Phishing	↑	↑	↑	↑	↑	↑	↑	↑
10. Spam	→			↑				↑
11. Rogueware/ Ransomware/ Scareware	↑							
12. Data Breaches	↑		↑		↑	↑	↑	↑
13. Information Leakage	↑	↑	↑	↑	↑	↑	↑	↑
14. Targeted Attacks	↑	↑				→	↑	↑
15. Watering Hole	↑							

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

La figura siguiente muestra la participación de los diferentes agentes considerados en el despliegue de las principales amenazas identificadas.

	Threat Agents								
	Corporations	Nation States	Hacktivists	Cyber Terrorists	Cyber Criminals	Cyber Fighters	Script Kiddies	Online Social Hackers	Employees
Drive-by exploits		✓			✓				
Worms/Trojans		✓		✓	✓	✓		✓	✓
Code Injection	✓	✓	✓	✓	✓	✓	✓		
Exploit kits			✓	✓	✓	✓	✓		
Botnets	✓	✓	✓	✓	✓	✓			
Physical Damage/ Theft/ Loss	✓	✓	✓	✓	✓	✓	✓	✓	✓
Identity Theft/. Fraud	✓	✓	✓	✓	✓	✓	✓	✓	✓
Denial of service		✓	✓	✓	✓	✓	✓		✓
Phishing	✓	✓			✓			✓	
Spam	✓				✓			✓	
Rogueware/ Ransomware/ Scareware					✓				
Data Breaches	✓	✓	✓	✓	✓	✓	✓		✓
Information Leakage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Targeted Attacks	✓	✓	✓	✓	✓	✓		✓	
Watering Hole	✓[175]	✓			✓	✓			

8.2 La Estrategia Europea de Ciberseguridad

En 2013 se publicó la Estrategia de Ciberseguridad de la UE (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013)[141]. Se trata del primer documento elaborado en este ámbito y comprende los aspectos del mercado interior, justicia y asuntos de interior y política exterior relacionados con el ciberespacio.

La Estrategia va acompañada de una propuesta legislativa técnica (Directiva) de la Dirección General de Redes de Comunicación, Contenido y Tecnologías de la Comisión Europea para reforzar la seguridad de los sistemas de información de la UE (Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - COM(2013) 48 final - 7/2/2013)[142]. Ambas iniciativas persiguen aumentar la confianza de los ciudadanos a la hora de utilizar Internet y comprar productos online, fomentando el crecimiento económico.

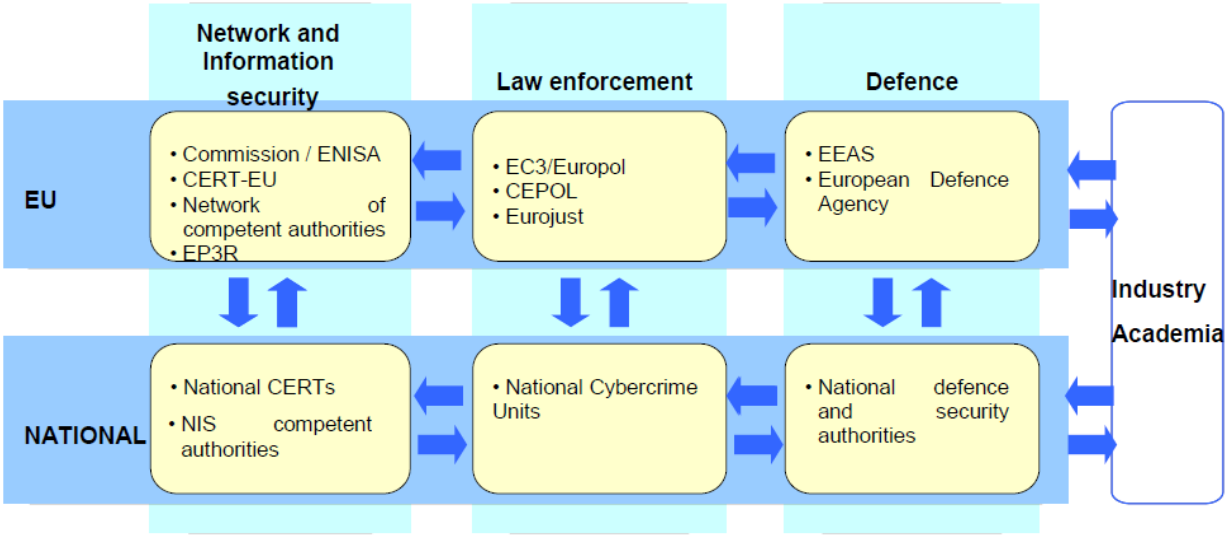
La Estrategia presenta las prioridades de la política internacional de la UE en relación con el ciberespacio:

- Libertad y apertura: la estrategia destaca la visión y los principios de la aplicación en el ciberespacio de los valores esenciales de la UE y los derechos fundamentales.

141 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

142 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666

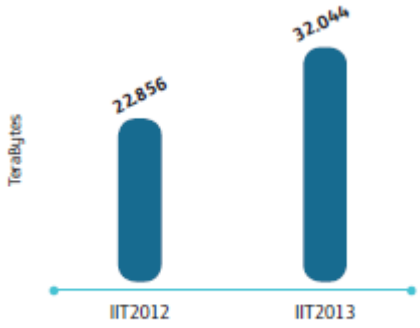
- Las leyes, normas y valores esenciales de la UE se aplican tanto en el ciberespacio como el mundo físico: la responsabilidad de velar por un ciberespacio más seguro corresponde a todos los actores de la sociedad de la información, desde los ciudadanos a los gobiernos.
- Desarrollo de la creación de capacidades de ciberseguridad: la UE se comprometerá con los socios y las organizaciones internacionales, el sector privado y la sociedad civil a apoyar la creación general de capacidades en terceros países, que incluirá la mejora del acceso a la información y a una Internet abierta y la prevención de ataques cibernéticos.
- Impulso de la cooperación internacional en aspectos del ciberespacio.



9. LA CIBERSEGURIDAD EN ESPAÑA

En cifras absolutas, 24,8 millones de españoles acceden a Internet entre la población de 16 y 74 años[143] (700.000 más que en 2012), es decir el 71,6% de dicho segmento. Nuestro país se encuentra a la cabeza en el desarrollo del **mercado móvil**, incluido el Internet móvil. Así, ya en el año 2010 el 13% de los españoles se conectaban a **Internet mediante el móvil** frente al 8% de los europeos. Y en la actualidad los datos siguen mostrando una considerable diferencia a favor de España: 57% de los usuarios de móvil se conectan a Internet en nuestro país en el año 2013 frente al 49% de los europeos. Ello supone una mayor presión para las redes móviles de telefonía que han visto de esta manera como el número de líneas móviles conectadas a Internet (tanto de terminales móviles como de datacards) aumentaba un 43% en el último año mientras el tráfico de datos cursado por dichas líneas lo hacía en un 40%3 (datos del 2T de 2013).

Se observa también un aumento en el consumo del servicio de datos, tanto fijos como móviles (véase figura). El aumento de dispositivos que se conectan a Internet como las tablets, televisiones y smartphones, así como el acceso a contenidos más pesados, principalmente audiovisuales, es más que palpable.



Fuente: CMT.

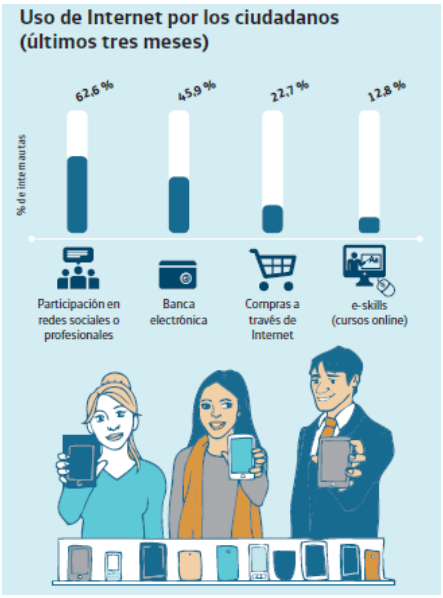
Tráfico de datos redes móviles

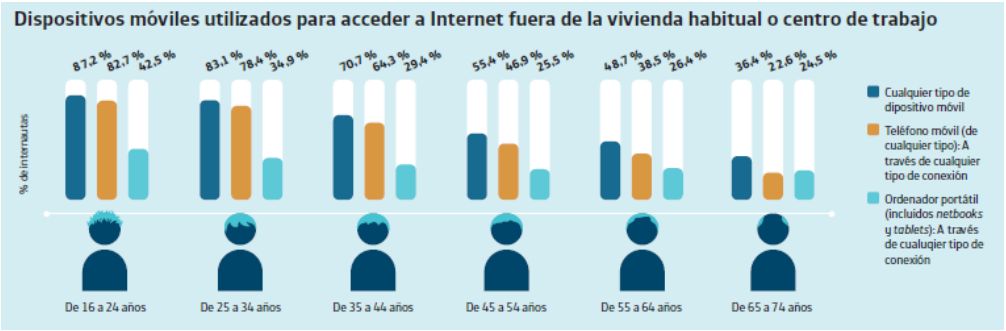
Según estas mismas fuentes, si 2012 se caracterizó por el notable incremento en la penetración de los smartphones, en 2013 los protagonistas han sido los tablets, ya que por primera vez se espera que a finales de ese año la venta de tablets supere a la de ordenadores portátiles.También destacaron los datos del comercio electrónico, con un incremento del 15,1% en el primer trimestre de 2013, hasta alcanzar los 2.822,6 millones de euros de volumen de negocio.De hecho, en torno a 13 millones de personas (un 37,4% de la población de 16 a 74 años) han realizado operaciones de comercio electrónico alguna vez en su vida.

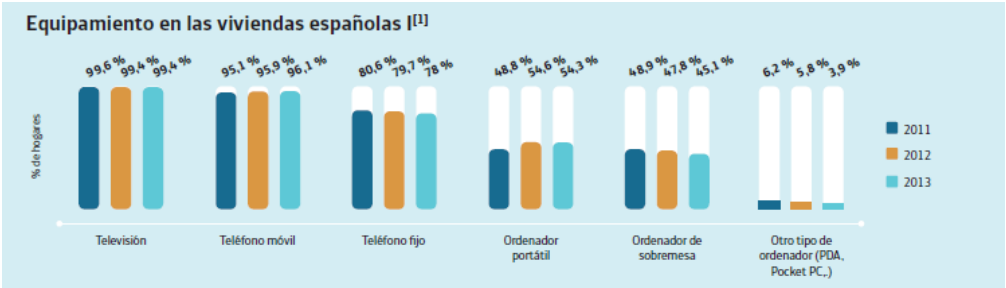
En cuanto a las redes sociales, el 64,1% de los usuarios de Internet en los últimos tres meses participa en redes sociales de carácter general (Facebook, Twitter o Tuenti) creando un perfil de usuario o enviando mensajes. Por otra parte, el 14,6% de los internautas ha

[143] Informe Telefónica-Sociedad de la Información España 2013

participado en redes de tipo profesional, como Linkedin o Xing. Este porcentaje se incrementa en el caso de trabajadores relacionados con el sector TIC (47,1%) y en el caso de los titulados superiores (29,3%). Los gráficos siguientes se han extraído del Informe sobre la Sociedad de la Información en España, de Telefónica.







Administración pública

No es ya ninguna novedad que la Administración pública es uno de los principales motores de impulso de la economía digital y que sus servicios y trámites son, cada vez más, realizados por medios telemáticos. Así y según el Ministerio de Hacienda y

Administraciones Públicas y su Sistema de Información Administrativa (SIA)[144], los trámites que los ciudadanos y las empresas realizaron con la Administración General del Estado, AGE, en 2013 superaron los 480 millones, de ellos, más de 367 millones (76,5%) se llevaron a cabo por vía electrónica (frente al 74,4% de 2012). De los trámites con la AGE, para las empresas, representan ya el 93,96% frente al 65,08% para los ciudadanos.

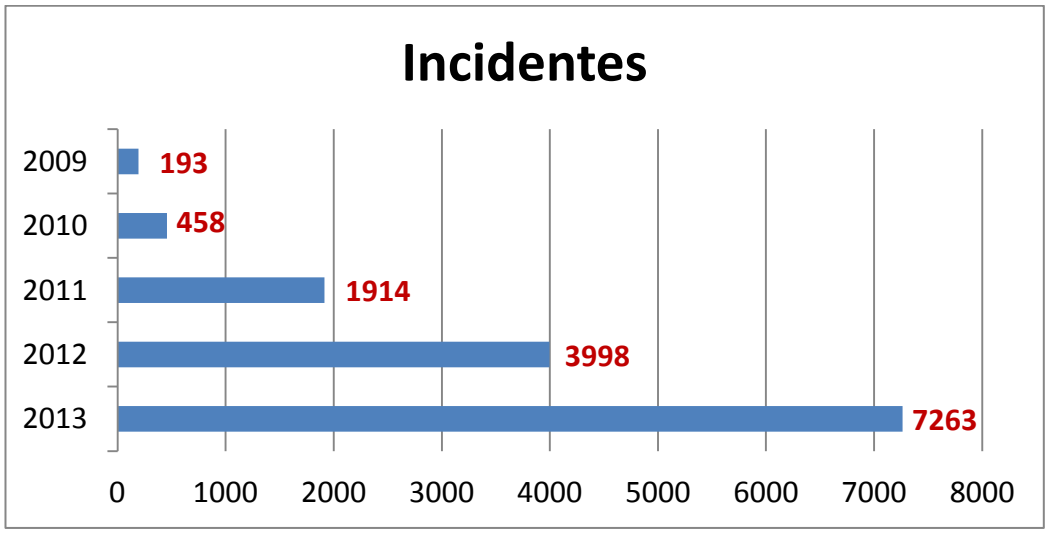
Volumen de trámites (especial atención) por tipo		Trimestre 1	Trimestre 2	Trimestre 3	Trimestre 4	Total
2013	1. Volumen Trámites Electrónicos	94.061.299	103.426.873	84.097.933	85.854.334	367.440.439
	- Volumen Trámites Electrónicos (Otros)	91.555.754	100.706.102	81.624.269	83.379.201	357.265.326
	- Volumen Trámites Certificado	2.505.545	2.720.771	2.473.664	2.475.133	10.175.113
	* Volumen Trámites DNIe	17.817	20.794	14.241	17.676	70.528
	2. Volumen Trámites No Electrónicos	25.783.256	40.793.616	25.573.621	20.484.447	112.634.940
	Total 2013	119.844.555	144.220.489	109.671.554	106.338.781	480.075.379
2012	1. Volumen Trámites Electrónicos	93.883.455	99.722.874	81.685.967	84.787.916	360.080.212
	- Volumen Trámites Electrónicos (Otros)	93.480.737	97.734.822	79.524.647	82.497.859	353.238.065
	- Volumen Trámites Certificado	403.718	1.988.052	2.161.320	2.290.057	6.842.147
	* Volumen Trámites DNIe	6.149	10.624	11.250	12.357	40.380
	2. Volumen Trámites No Electrónicos	29.695.831	41.334.502	25.969.819	26.682.550	123.682.702
	Total 2012	123.579.286	141.057.376	107.655.786	111.470.466	483.762.914
2011	1. Volumen Trámites Electrónicos	75.253.583	116.125.855	81.536.964	82.241.142	355.157.544
	- Volumen Trámites Electrónicos (Otros)	74.530.252	114.933.279	80.620.846	81.537.021	351.621.398
	- Volumen Trámites Certificado	723.331	1.192.576	916.118	704.121	3.536.146
	* Volumen Trámites DNIe	106	3.077	3.731	1.368	8.282
	2. Volumen Trámites No Electrónicos	28.025.167	46.998.362	30.781.858	25.743.429	131.548.816
	Total 2011	103.278.750	163.124.217	112.318.822	107.984.571	486.706.360

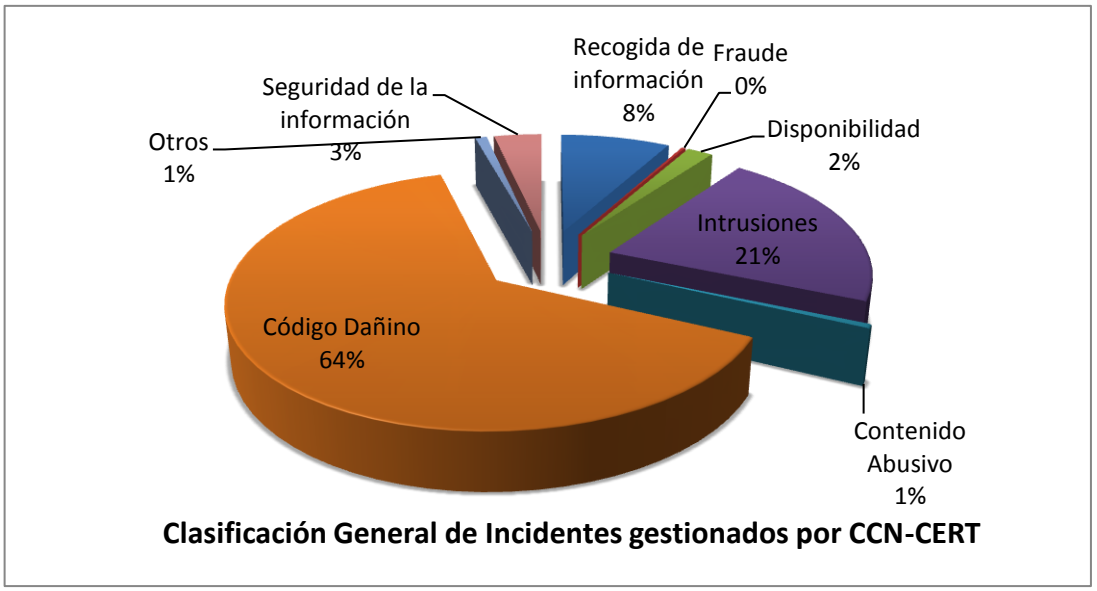
9.1 Incidentes gestionados por el CCN-CERT

Ante este grado de penetración de Internet en nuestra sociedad, no es de extrañar que se incremente el número de amenazas e incidentes sobre los sistemas de nuestra Administración, empresas y ciudadanos. Prueba de ello, es el número de incidentes gestionados por el CCN-CERT. Estos incidentes se produjeron contra los sistemas de las Administraciones Públicas españolas y sobre empresas y organizaciones de interés estratégico nacional. En total, durante 2013, el CERT Gubernamental gestiónó un total de 7.260 incidentes, frente a los 3.998 del ejercicio anterior. De ellos, 4.899 fueron catalogados por el Equipo de expertos del CERT Gubernamental con una criticidad entre de alto (3.829), muy alto (1.032) y crítico (38).

De ellos, el 64% de los incidentes fueron motivados por código dañino; el 21% fueron intrusiones en los sistemas y el 8% de los denominados como recogida de información (fase inicial de los ataques).

[144] http://www.minhap.gob.es/es-ES/Prensa/Documents/20140309_SIA.pdf





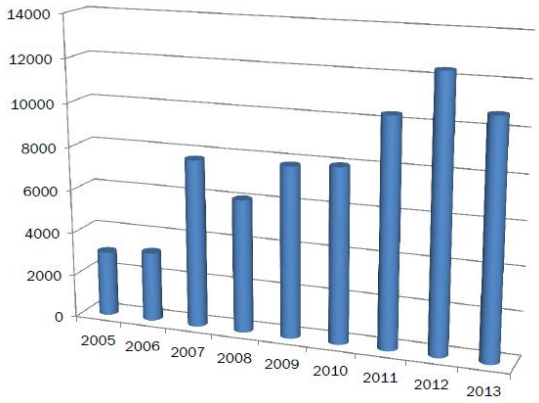
Clasificación General de Incidentes gestionados por CCN-CERT

9.2 Vulnerabilidades gestionadas por el CCN-CERT

En el desarrollo de una de sus funciones relacionadas con el Esquema Nacional de Seguridad, el CERT gubernamental (CCN-CERT)[145] gestionó un total de 10.714 vulnerabilidades, una cifra ligeramente inferior a la registrada en 2012.

La figura siguiente muestra la evolución anual de esta gestión de vulnerabilidades.

145 https://www.ccn-cert.cni.es/



Evolución anual de las vulnerabilidades gestionadas por el CCN-CERT

Las vulnerabilidades gestionadas tuvieron el nivel de riesgo que se indica en el cuadro siguiente.

Nivel ALTO	**2.783**
Nivel MEDIO	**4.214**
Nivel BAJO	**3.717**
Total	**10.714**

9.3 Marco normativo

9.3.1 Ley de Seguridad Privada

Aprobada por el Congreso de los Diputados el 20 de marzo de este mismo año (2014)[146] y a la espera de su publicación en el BOE, la nueva Ley de Seguridad Privada sustituye a la norma vigente desde el año 1992. Esta nueva ley menciona la seguridad de la información y las comunicaciones, por primera vez configurada no como actividad específica de seguridad privada, sino como actividad compatible (artículo 6) y señala que "A las empresas, sean o no de seguridad privada, que se dediquen a las actividades de seguridad informática, entendida como el conjunto de medidas encaminadas a proteger los sistemas de información a fin de garantizar la confidencialidad, disponibilidad e integridad de la misma o del servicio que aquéllos prestan, por su incidencia directa en la seguridad de las entidades públicas y privadas, se les podrán imponer reglamentariamente requisitos específicos para garantizar la calidad de los servicios que presten".

[146] http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-50-5.PDF

Del mismo modo, y dentro del capítulo de infracciones muy graves, la citada Ley menciona como tal "La falta de comunicación por parte de empresas de seguridad informática de las incidencias relativas al sistema de cuya protección sean responsables cuando sea preceptivo".

9.3.2 Protocolo al Convenio sobre la Ciberdelincuencia para penalizar de índole racista y xenófoba

Durante 2013, el Consejo de Ministros autorizó la firma del Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Con ello se armoniza el derecho de los Estados miembros y de los demás estados firmantes, y se amplía el ya firmado y ratificado por España Convenio sobre ciberdelincuencia.

El objetivo del Protocolo es la asistencia mutua en dos aspectos: uno, la armonización de la legislación penal sustantiva en cuanto a la lucha contra el racismo y la xenofobia en Internet y, otro, en cuanto a mejora de la cooperación internacional en esta área.

En cuanto a las medidas que deben tomarse a nivel nacional, las partes firmantes deberán tomar medidas legislativas o de otra índole para evitar la difusión de material racista y xenófobo mediante sistemas informáticos, impedir que mediante las redes se den amenazas o insultos con motivación racista o xenófoba y también impedir que se utilicen sistemas informáticos para negar o justificar genocidios o crímenes contra la humanidad.

9.3.3 Subcomisión sobre Redes Sociales en el Congreso de los Diputados

La Comisión de Interior del Congreso, en su sesión del día 27 de febrero de 2013, acordó crear esta Subcomisión con el objeto de analizar la situación actual en España respecto a las Redes Sociales.

Analizar la situación en países de nuestro entorno, estudiar el papel que las administraciones públicas tienen en el mundo de las redes sociales e intensificar la cooperación e intercambio de información con los administradores de las redes sociales, mediante la activación de canales de comunicación ágiles, son algunos de los objetivos de la Subcomisión.

Del mismo modo, determinará qué modificaciones legislativas se deben llevar a cabo para mejorar la protección integral de nuestros menores y la educación en su utilización, así como las medidas necesarias para la protección de los derechos de propiedad intelectual en el entorno de las redes sociales y para la promoción de conductas respetuosas con estos derechos por parte de los usuarios de las citadas redes.

9.3.4 Agenda Digital

Se aprobó en 2013, en línea con los objetivos de la Agenda Digital Europea, con el fin de trasladar los beneficios de las nuevas tecnologías a ciudadanos, empresas y Administraciones.

9.3.5 Proyecto de Ley General de Telecomunicaciones

Se encuentra en estos momentos en trámite parlamentario (en el Senado), por lo que su aprobación definitiva se espera para este año 2014.

9.3.6 Modificación del RD 3/2010 Esquema Nacional de Seguridad

Se encuentra en estos momentos en fase de recepción de comentarios por pare de la Administración General del Estado.

9.4 El hackitivismo en España

El hacktivismo en España durante 2013 se ha mantenido principalmente expresado a través de Anonymous, aunque con sensibles variaciones en cuanto a organización y actividad con respecto a 2011 y 2012.

En años anteriores, la actividad de Anonymous en España estaba canalizada a través de una facción con denominación nacional (#OpSpain), una organización interna que se articulaba fundamentalmente a través de ciberidentidades que se comunicaban en salas de IRChat, y operaciones específicas.

De una facción nacional a pequeñas células con nombre propio

En España y en lo que al conglomerado Anonymous se refiere, durante los dos últimos meses de 2012 se inició la actividad, de pequeñas cibercélulas que ejecutan ataques puntuales. La 9ª Compañía de Anonymous y Lulzes representaban a principios de 2013 el componente ciberofensivo de Anonymous en España, sin que haya logrado reconstituirse, de momento, una facción de marca nacional a partir de la desmembrada #OpSpain. Hasta cinco identidades estuvieron operando durante el arranque de 2013. Estas tienen en común la especialización en ciberataques aprovechando vulnerabilidad XSS y una cierta órbita alrededor de Anonymous en Barcelona.

En el inicio de 2013 se verificó el intento de constituir un renacimiento de una marca nacional de Anonymous en España a través de una célula con algunos elementos periféricos del antiguo grupo #OpSpain y denominándola Anonymous España. Aunque llegó a establecerse una mínima estructura y una infraestructura con canales de comunicación e identidades en redes sociales, incluso un atisbo de operación propia, el nuevo grupo no fructificó.

Como contraposición a la ausencia de en una facción nacional de Anonymous en España, en el último trimestre de 2013 se detectaron intentos por parte de ciberidentidades que como Black Knights o Lulz Security España pretenden llenar un espacio en la vanguardia de Anonymous en España que actualmente está ocupado en términos operativos, por La 9ª Compañía de Anonymous. Estos intentos son incipientes; muestran una denominación e iconografía que trata de proyectar la imagen de que son identidades grupales, aunque sea probable que estén constituidas por una sola persona; intentan incorporar algún componente latinoamericano; y además de actividad de propaganda pueden tener capacidad técnica, como máximo, para producir ataques por inyección XSS. De momento su evaluación como amenaza es baja.

Dos únicas ciberoperaciones activas

A pesar de que durante 2013 se han registrado intentos de llevar adelante operaciones de Anonymous en España al estilo clásico (bautizo con nombre, construcción de narrativa militante y producción de contenido multimedia para apoyarla, constitución de perfiles de propaganda en redes sociales), la ausencia de una facción nacional aglutinante y liderando las operaciones ha llevado a la práctica ausencia de marcos de ciberataque organizados y sostenidos en el tiempo.

Durante los dos meses primeros meses de 2013, la única operación estable de Anonymous en España, con considerable actividad además, fue la #OpDesahucios, un marco de ciberataque que correlacionaba con la narrativa militante de grupos reivindicativos (plataforma 'Stop Desahucios') que demandan la anulación de las órdenes de desahucio sobre familias desprovistas de recursos económicos y que no pueden hacer frente al pago de préstamos hipotecarios. Al menos durante el primer tercio de 2013, la ciberidentidad Anonymous Vendetta fue la protagonista más activa de los ataques en el marco de la #OpDesahucios, la mayoría contra webs locales del Partido Popular o contra empresas inmobiliarias y teniendo la inyección XSS como mecanismo de ciberataque preferente, con alguna explotación ocasional de vulnerabilidades SQL sobre servidores web.

La #OpDesahucios comenzó con sostenida actividad pero fue paulatinamente decayendo a lo largo del primer semestre del año. Tras el letargo de la actividad de identidades Anonymous en España en el verano de 2013, en el último trimestre del año se constituyó la #OpOpusDei, una narrativa de ciberataque enfocada principalmente contra webs del Partido Popular, de la Iglesia Católica y de centros educativos que los promotores de la operación identificaban con colectivo católico Opus Dei.

La #OpOpusDei se desarrolló en octubre y noviembre de 2013. Fue ejecutada por ciberidentidades constituidas en redes sociales (Facebook y Twitter) adoptando el propio nombre de la operación y desplegando ataques mediante la explotación de vulnerabilidades XSS y SQL sobre las webs objetivo.

Leves indicadores de sinergia entre activismo y hacktivismo

En una aproximación preliminar al análisis en España de la convergencia entre militancias antisistema y empleo de tecnologías de la información tanto para ciberatacar objetivos como para organizar la actividad militante en un ecosistema que ha venido en llamarse 'hacktivismo', se constata la existencia de un núcleo de 'hacktivistas' todavía poco compacto; vinculados a colectivos en el tejido 'indignado', 15M o la 'Plataforma de Afectados por la Hipoteca'; y con procedencia de los antiguos hacklabs de los circuitos ciberpunks, están actualmente orbitando alrededor del movimiento libertario en Madrid o Barcelona.

Este tejido hacktivista está comenzando a desarrollar aplicaciones con software libre en principio para apoyar movimientos reivindicativos (como la PAH), para apoyar acciones de acoso (como la operación del 15M madrileño #ToqueABankia contra la entidad bancaria del mismo nombre) pero principalmente para poner a disposición del activismo herramientas de cifrado que protejan sus comunicaciones. Esta línea de acción ha comenzado a manifestarse, en términos prácticos, en la organización de las reuniones CryptoParty.

Expresión de ese patrón de sinergia entre activistas sobre el terreno físico y hacktivistas en el terreno cibernético fue el marco militante #ToqueABankia que organizado por una célula del movimiento 15M en Madrid durante el primer trimestre de 2013, consistió en lo que fue denominado como un (ataque distribuido por denegación de servicio) DDoS físico o como una 'movilización ciudadana distribuida masiva' o 'acción XSwarm': el intento de ocupación masivo y coordinado de oficinas de Bankia en todo el territorio nacional por parte de activistas cuyo propósito era ralentizar y bloquear el normal funcionamiento de las sucursales demandando multitud de microtareas como si fueran usuarios ordinarios de los servicios bancarios. En paralelo al activismo en el plano físico, #ToqueABankia dispuso de un considerable soporte organizativo en web diseñado y desarrollado por identidades adscritas a colectivos 'hacktivistas', varios de ellos vinculados con hacklabs a su vez asociados a los denominados centros sociales autogestionados (CSO) de orientación 'okupa' y libertaria.

En este incipiente plano de intersección entre activismo y hacktivismo en España, durante 2013 se materializaron un par de escenarios en donde se produjeron difusiones de documentos por procedimientos a los que se pretendió otorgar la apariencia 'Anonymous', pero ni el origen de la documentación difundida procedía de actividades de hacking en sentido de ciberseguridad ni los canales empleados para la difusión concuerdan con la topografía de una operación de 'Anonymous'.

El primero de los escenarios fue el denominado #PPGoteras en julio de 2013, que consistió en la difusión de documentos contables atribuidos al Partido Popular y aparentemente presentados ante el Tribunal de Cuentas. El segundo de los escenarios involucró la filtración en octubre de 2013, vía redes sociales, de informes de operaciones atribuidos al Centro de Seguridad de la Información de Cataluña (CESICAT), un órgano de naturaleza parcialmente pública. Los informes divulgados en la que fue denominada como #OPGovCAT detallaban la supuesta monitorización que medios atribuidos al Cesicat habrían venido realizando de perfiles en redes sociales presuntamente relacionados con colectivos activistas y hacktivistas en España.

Vector islamista/nacionalista

Aunque no conformando un patrón estable a lo largo de 2013, sí es este año cuando se observa intencionalidad, narrativa y al menos un mínimo de organización para coordinar ciberataques contra webs en el ciberespacio español, desde ciberidentidades con iconografía árabe y adoptando una simbología que mezclaba contenidos islamistas con reivindicaciones nacionalistas respecto del Sáhara y Ceuta-Melilla. Esta expresión de conglomerados de ciberidentidades árabes que lanzan oleadas sincronizadas de ataques contra webs en países no árabes en base a una narrativa militante islamista/nacionalista ha tenido en 2013 expresión también en el ámbito internacional, además de en España.

En el escenario español, en abril de 2013 y en el marco de una narrativa de ataque al ciberespacio español reivindicando la marroquinidad del Sáhara y de las ciudades de Ceuta y Melilla, ciberidentidades referenciadas a Marruecos desplegaron ataques contra webs españoles en un par de fases, primero bajo la denominación de #OpEspagne/#OpSpain bajo la dirección de 'Moroccan Anonymous'; y después bajo la nomenclatura 'Operación Nuevos Conquistadores', organizada por 'Moroccan Islamic Union-mail'.

Durante la ofensiva se atacaron principalmente webs de bajo perfil y alta vulnerabilidad, aunque en gran número. Todos los ataques fueron por deface con inyecciones de varias composiciones gráficas con imágenes/mensajes antiespañoles y alusivos a la narrativa de la operación. Los grupos más activos fueron 'Moroccan Ghosts', 'Moroccan Islamic Union-mail' y 'Moroccan Hackers PRO'.

9.5 La Estrategia de Seguridad Nacional de 2013

En 2013, el Consejo de Ministros aprobó la **Estrategia de Seguridad Nacional de 2013** y un Real Decreto, que modifica otro de 2011, que establecía las Comisiones Delegadas del Gobierno, todo ello con el fin de incluir entre las mismas al **Consejo de Seguridad Nacional** en su condición de Comisión Delegada para la Seguridad Nacional. Este Consejo de Seguridad Nacional está presidido por el Presidente del Gobierno.

La Estrategia persevera en el enfoque integral de la Seguridad Nacional. En este sentido, se contempla el concepto de seguridad de una manera amplia acorde con estas transformaciones globales que afectan al Estado y a la vida diaria del ciudadano. La seguridad comprende ámbitos muy diversos y el carácter esencialmente transnacional y transversal de los riesgos y amenazas que comprometen la seguridad en nuestros días demandan respuestas completas.

Ámbitos de actuación

La Estrategia contempla hasta doce riesgos para la seguridad del Estado: conflictos armados; terrorismo; ciberamenazas; crimen organizado; inestabilidad económica y financiera; vulnerabilidad energética; flujos migratorios irregulares; armas de destrucción masiva; espionaje; emergencias y catástrofes naturales; vulnerabilidad del espacio marítimo y vulnerabilidad de las infraestructuras críticas y servicios esenciales.

Esta Estrategia es una revisión de la Estrategia aprobada en 2011 por el anterior Ejecutivo, y que cuenta con el respaldo político del principal partido de la oposición. El objetivo del Gobierno es reforzar y hacer extensible a todos, este consenso político y social, porque se trata de una verdadera política de Estado.

Estructura de la Estrategia

En lo relativo a la estructura de la Estrategia, el documento cuenta con cinco capítulos:

- El capítulo 1 ofrece un concepto de Seguridad Nacional integral acorde con los riesgos y amenazas actuales.
- El capítulo 2 sitúa la seguridad de España en el mundo y presenta las grandes prioridades estratégicas de España como Estado diverso y plural.
- El capítulo 3 identifica los principales riesgos y amenazas para la Seguridad Nacional.
- El capítulo 4 define los ámbitos de actuación prioritarios en materia de Seguridad Nacional a la luz de los riesgos y amenazas que nos afectan.

- El capítulo 5 define el Sistema de Seguridad Nacional que potenciará la actuación coordinada de las Administraciones en un uso eficiente y racional de los recursos actuales.

Además, la Estrategia prevé un sistema institucional flexible para potenciar la actuación coordinada de los instrumentos existentes en el campo de la seguridad. Este sistema estará liderado por el presidente del Gobierno y se apoyará en el nuevo Consejo de Seguridad Nacional, que será un órgano colegiado del Gobierno, que responde al Programa de Reformas del Gobierno y que nace con la vocación de administrar de una forma más eficaz y eficiente los recursos existentes.

Composición del Consejo de Seguridad Nacional

El presidente del Gobierno lo presidirá, excepto cuando S.M. el Rey asista a sus reuniones. Se reunirá periódicamente, al menos una vez cada dos meses, y cuantas veces lo demanden las circunstancias. Además de la Presidencia, el Consejo estará compuesto por los siguientes miembros:

- Vicepresidente del Gobierno
- Ministro de Asuntos Exteriores y Cooperación
- Ministro de Defensa
- Ministro de Hacienda y Administraciones Públicas
- Ministro de Interior
- Ministro de Fomento
- Ministro de Industria, Energía y Turismo
- Ministro de Economía y Competitividad
- Director del Gabinete de la Presidencia del Gobierno, que actuará como secretario.
- Secretario de Estado de Asuntos Exteriores
- Jefe de Estado Mayor de la Defensa
- Secretario de Estado de Seguridad
- Secretario de Estado Director del Centro Nacional de Inteligencia
- Responsable del Departamento de Seguridad Nacional

Este Consejo equipara a España a países de su entorno donde existen órganos similares, que se reúnen regularmente para discutir colectivamente los objetivos del Gobierno en esta materia y para gestionar crisis que requieren una participación multisectorial.

Para una mejor operatividad, el Consejo de Seguridad Nacional tiene el mandato de elaborar una propuesta de Anteproyecto de Ley Orgánica de Seguridad Nacional para su posterior elevación al Consejo de Ministros

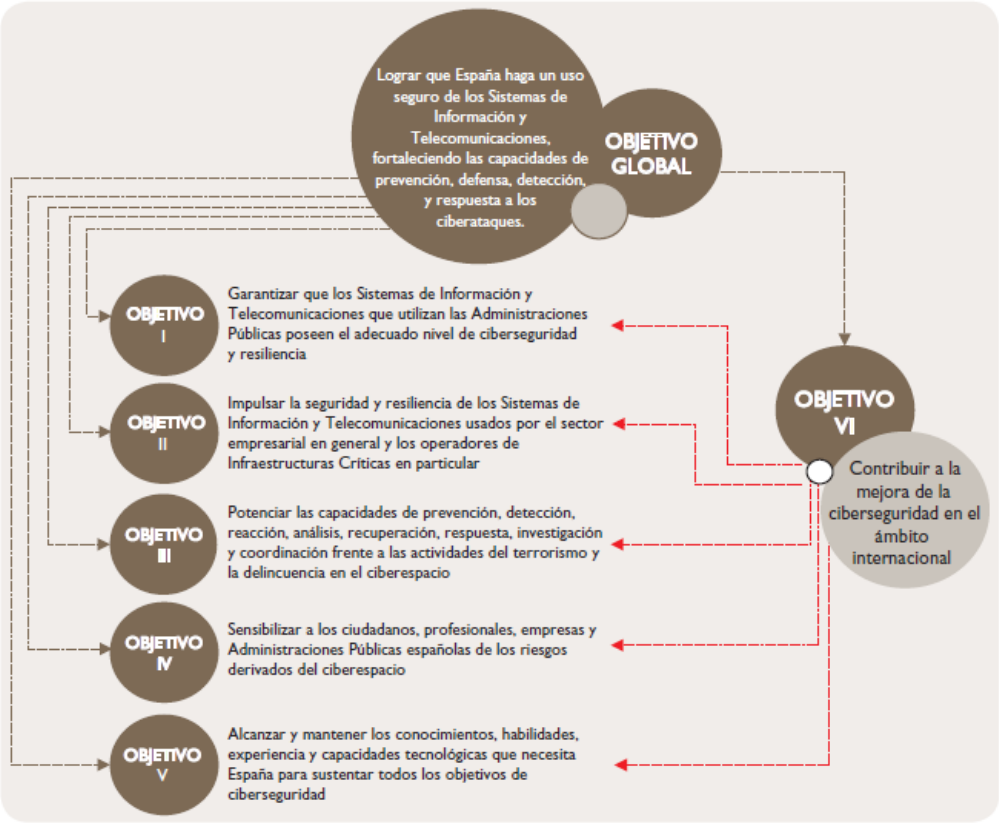
9.6 La Estrategia de Ciberseguridad Nacional

Como así ha sido señalado por el Presidente del Gobierno, el Consejo de Seguridad Nacional, plenamente consciente de la importancia de la cuestión y comprometido con el desarrollo de la Sociedad Digital, impulsó en 2013 la elaboración de **la Estrategia de Ciberseguridad Nacional** con el fin de dar respuesta al enorme desafío que supone la preservación del ciberespacio de los riesgos y amenazas que se ciernen sobre él.

Así pues, la Estrategia de Ciberseguridad Nacional se adopta al amparo y alineada con la Estrategia de Seguridad Nacional de 2013, que contempla la ciberseguridad dentro de sus doce ámbitos de actuación.

En anexo E se incluye el texto correspondiente a su Resumen Ejecutivo.

La figura siguiente muestra un esquema de los Objetivos de la ECSN.



Durante el primer año, el Comité Especializado de Ciberseguridad estará presidido por el Ministerio de la Presidencia, a través del Centro Nacional de Inteligencia.

9.7 El Esquema Nacional de Seguridad

9.7.1 Situación actual del ENS

El 30 de enero de este año 2014, concluía el plazo de 48 meses fijado por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica para la adecuación de los sistemas de las AAPP a dicho Esquema.

Durante el año 2013 se realizó un seguimiento estrecho del progreso de la adecuación al ENS, por parte del Ministerio de Hacienda y Administraciones Públicas, conjuntamente con el Centro Criptológico Nacional (CCN), en la Administración General del Estado, para conocer el estado de situación de dicho progreso e identificar los aspectos de mayor dificultad. Aunque cabría esperar un mayor grado de avance, existen diversos aspectos que sí se encuentran entre los baremos aceptables. En cualquier caso ha de tenerse en cuenta que el esfuerzo de

adecuación al ENS se ha venido realizando en condiciones que suponen un esfuerzo notable por la limitación de recursos económicos y humanos en las que se desenvuelve la actividad de las entidades de la Administración.

En este sentido se han publicado las siguientes Guías CCN-STIC, monográficamente dirigidas al ENS:

Guía 800 - Glosario de Términos y Abreviaturas del ENS	03-2011
Guía 801 - Responsables y Funciones en el Esquema Nacional de Seguridad	02-2011
Guía 802 - Auditoría del Esquema Nacional de Seguridad	06-2010
Guía 803 - Valoración de sistemas en el Esquema Nacional de Seguridad	01-2011
Guía 804 - Medidas de implantación del Esquema Nacional de Seguridad	03-2013
Guía 805 - Política de Seguridad de la Información	09-2011
Guía 806 - Plan de Adecuación del Esquema Nacional de Seguridad	01-2011
Guía 807 - Criptología de empleo en el Esquema Nacional de Seguridad	11-2012
Guía 808 - Verificación del cumplimiento de las medidas en el ENS	09-2011
Guía 809 - Declaración de Conformidad del Esquema Nacional de Seguridad	07-2010
Guía 810 - Creación de un CERT / CSIRT	09-2011
Guía 811 - Interconexión en el Esquema Nacional de Seguridad	11-2012
Guía 812 - Seguridad en Entornos y Aplicaciones Web	10-2011
Guía 813 – Componentes certificados en el ENS	02-2012
Guía 814 - Seguridad en correo electrónico	08-2011
Guía 815 - Métricas e Indicadores en el Esquema Nacional de Seguridad	07-2013
Guía 817 – Criterios comunes para la Gestión de Incidentes de Seguridad	08-2012
Guía 818 – Herramientas de Seguridad en el ENS	10-2012
Guía 820 – Protección contra Denegación de Servicio	06-2013
Guía 821 – Normas de Seguridad en el ENS	04-2013
Guía 822 – Procedimientos de Seguridad en el ENS	10-2012
Guía 823 – Seguridad en entornos Cloud	06-2013
Guía 824 – Informe del Estado de Seguridad	11-2012
Guía 825 – ENS & 27001	11-2013

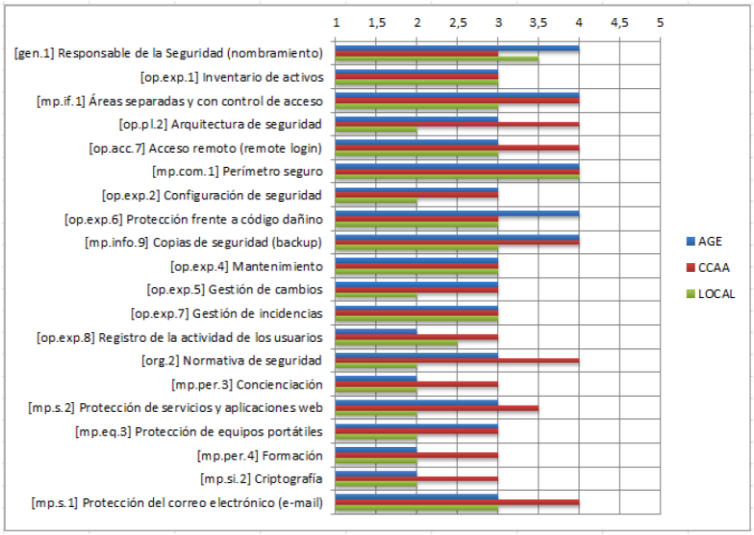
Además, el Centro Criptológico Nacional ha desarrollado diversos programas de apoyo (herramientas PILAR 5.2.3 y µPILAR 5.2.3)

9.7.2 Seguimiento en las AA.PP.

- Acuerdos de la Comisión Permanente del Consejo Superior de Administración Electrónica y del Comité de Seguridad de la Información de las AA.PP.
- Seguimiento: febrero (sólo AGE), mayo, septiembre y diciembre de 2013.
- Participación de carácter voluntario.

	feb	jun	sep
AGE	60	65	71
AYTO	2	12	13
CCAA	5	27	29
Diputacion		5	6
	67	109	119

No todas las medidas de seguridad señalas en el ENS han gozado del mismo nivel de adaptación por parte de los organismos públicos. La figura siguiente muestra una panorámica de una selección de medidas, en base a datos de septiembre de 2013:



A la luz de estos datos se entiende que, al cierre de 2013, el grado de avance debería ser mayor, aunque se está haciendo un esfuerzo considerable.

De cara a disponer de unas Administraciones públicas adaptadas lo antes posible al ENS, se han enfatizado una serie de medidas a corto plazo, entre las que destacan:

- Existencia de un Plan de Adecuación.
- Existencia de un Responsable de Seguridad nombrado.
- Exista una categorización de los sistemas de información afectados por el ENS.
- Se realice el análisis de riesgos.
- Se aborden aspectos que tienen una componente mayor de gobernanza y documentación:
  - proceso de autorización,
  - arquitectura de seguridad
- Se apliquen las guías CCN-STIC para:
  - configuración de seguridad.
  - protección de aplicaciones web.

9.7.3 Evolución del ENS y retos inmediatos

Desde la fecha de entrada en vigor del ENS las amenazas han evolucionado, al tiempo que también lo han hecho las tecnologías.

En respuesta a todo ello, a la experiencia acumulada, a, los comentarios recibidos por distintos organismos, a la evolución regulatoria del contexto europeo e internacional y a lo dispuesto en el art. 42 del ENS, relativo a su actualización permanente, en la actualidad el ENS se encuentra en periodo de análisis de algunas modificaciones que persiguen una mejor, más eficaz y eficiente protección de los sistemas de información de los organismos de las AA.PP. españolas.

Las modificaciones previstas para el ENS pasarán por:

- Armonizar el modo común de actuar en relación con ciertas cuestiones.

- Regular la armonización en base a la promulgación de Normas Técnicas de Seguridad, aplicando los procedimientos consolidados en las Normas Técnicas de Interoperabilidad.
- Desarrollar la creación y penetración de las Guías CCN-STIC como mejores prácticas de aplicación e interpretación del ENS.
- Asentar un mecanismo periódico que permita recoger información para conocer e informar del estado de seguridad, en adecuadas condiciones de eficacia y eficiencia.
- Consolidar información de los incidentes y su notificación[147].
- Recopilación de las evidencias necesarias para la investigación como: registros de auditoría, configuraciones, soportes y otra información relevante[148].

Algunas de las medidas de seguridad que, presumiblemente, serán modificadas en 2014, serán:

- 3.4. Proceso de autorización [org.4]
- 4.1.2.Arquitectura de seguridad [op.pl.2]
- 4.1.5. Componentes certificados [op.pl.5] + medidas relacionadas
- 4.2.5. Mecanismo de autenticación [op.acc.5]
- 4.3.8. Registro de la actividad de los usuarios [op.exp.8]
- 4.6.1. Detección de intrusión [op.mon.1]
- 4.6.2. Sistema de métricas [op.mon.2]
- 5.4.3. Protección de la autenticidad y de la integridad [mp.com.3]
- 5.5.5. Borrado y destrucción [mp.si.5]
- 5.7.4. Firma electrónica [mp.info.4]
- 5.7.7 Copias de seguridad [mp.info.9]

A la vista del antedicho estado de situación del ENS, los retos inmediatos que se han considerado son los siguientes:

- Lograr la plena adecuación en condiciones de escasez de recursos humanos y materiales.
- La declaración de conformidad.
- Conocer e informar regularmente del estado de la seguridad de las AA.PP.
- Actualizar el ENS.
- Extender el ENS a todos los sistemas de información de las AA.PP.

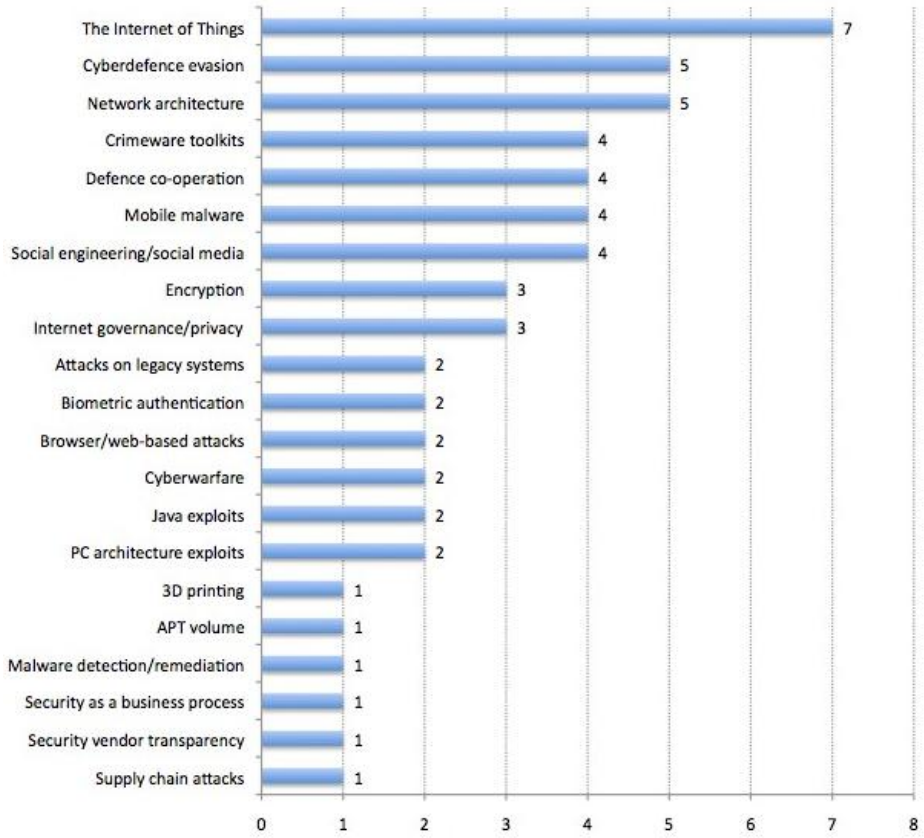
147 La práctica de la notificación de los hechos que tengan un impacto significativo en la seguridad es una tendencia en proyectos normativos de la UE.

148 Atendiendo, cuando resulte de aplicación, a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y su normativa de desarrollo.

PARTE II: TENDENCIAS 2014

10. TENDENCIAS 2014

Considerando las predicciones que han hecho varias de las empresas más representativas en materia de ciberseguridad, la figura siguiente muestra un ranking de las principales ciberamenazas para 2014[149].



Seguidamente, se desarrollan algunas de las tendencias más significativas que, atendiendo a la opinión de diferentes instituciones, empresas y reconocidos expertos, conformarán el entorno de la ciberseguridad en 2014.

Hemos dividido las tendencias en los siguientes 9 Grupos de Tendencias:

- Grupo de Tendencias I: Ciberespionaje y APTs.
- Grupo de Tendencias II: Código dañino.
- Grupo de Tendencias III: Dispositivos móviles.
- Grupo de Tendencias IV: Los servicios de ciberseguridad.
- Grupo de Tendencias V: Exploits y botnets.
- Grupo de Tendencias VI: Ataques contra sistemas operativos y navegadores.
- Grupo de Tendencias VII: Comportamientos institucionales y herramientas.
- Grupo de Tendencias VIII: Watering Hole y Cloud.
- Grupo de Tendencias IX: El hacktivismo.

149 Las empresas son: FireEye, Fortinet, Lancope, Neohapsis, Symantec, Websense y Zscaler.

10.1 Grupo de Tendencias I: Ciberespionaje y los APT

TENDENCIA I.1: La sofisticación operativa del ciberespionaje

A la vista de la evolución de este tipo de ataques en los últimos años, parece claro que el ciberespionaje continuará representando en 2014 la mayor ciberamenaza para las organizaciones, públicas o privadas, de todo el mundo, puesto que los atacantes seguirán madurando y mejorando sus modelos de ataque, así como revisando métodos y herramientas, para mejorar la eficacia de sus acciones y dificultar la detección y sobre todo su identificación.

Por ello, los atacantes implementarán controles de seguridad más estrictos en torno a sus operaciones. Se espera que sean más selectivos respecto de las víctimas, filtrando aquellos equipos que no cumplan con sus criterios. Por ello, se concentrarán en aquellos sistemas que constituyan sus objetivos, despreciando el resto.

Se espera además, que se incremente el uso de técnicas de ofuscación para limitar la capacidad de investigación y adquisición de inteligencia sobre los ataques.

Respecto a los canales de ex filtración de datos se seguirán empleando:

- Servicios Web (http y https).
- Servicio de correo electrónico.
- Servicio DNS.

En los servicios web, se incrementará el uso de sitios web comprometidos respecto a los que se encuentran bajo control total del atacante. El uso de DNS dinámico se mantendrá por las infraestructuras existentes. Estas técnicas permiten que el tráfico del atacante se mezcle con el tráfico web habitual permitirá pasando desapercibidos durante períodos más largos de tiempo. Por otro lado se incrementará el empleo de servicios en la nube (permitidos en muchas organizaciones) para el envío de información comprometida.

TENDENCIA I.2: Ataque a "objetivos blandos" para alcanzar el objetivo final

La madurez de las herramientas para detectar exploits, tales como el sandboxing y los antivirus de última generación, hará que la infección sea un poco más difícil para los atacantes que atacarán redes o dispositivos con menor nivel de seguridad, como paso intermedio para alcanzar la red que constituye el objetivo final. Estos, llamados, "objetivos blandos" incluyen redes de contratistas, proveedores y subsidiarias o equipos particulares de usuarios de estas redes como routers domésticos, televisores inteligentes y domótica.

TENDENCIA I.3: El uso de las redes sociales en las primeras fases de ataque

Durante la primera fase de los APT los atacantes realizan un reconocimiento previo para recabar inteligencia básica sobre su víctima potencial. En 2014, la observación de redes sociales profesionales (Linkedin) y personales (Facebook) se incrementará. La información

obtenida se usará para preparar coreos electrónicos dirigidos para comprometer la red corporativa objetivo[150].

TENDENCIA I.4: Las organizaciones incrementarán el uso de mecanismos de cifrado

Los problemas de privacidad han plagado los titulares de la prensa en 2013, llamando la atención de personas e instituciones sobre la enorme cantidad de información personal que (consciente o inconscientemente, consentidamente o no) se comparte y se trata diariamente. Es de esperar que, en 2014, los usuarios exijan a los proveedores de soluciones una mayor atención a la privacidad de sus datos. Muchos de ellos utilizarán herramientas como Tor de cara a ocultar su navegación en Internet[151].

Finalmente, a pesar de la expectación creada en torno a la capacidad para romper los algoritmos de cifrado por parte de los ordenadores cuánticos, es poco probable que el uso de la criptografía se altere de forma inmediata.

En 2014, se prevé un aumento en el uso del cifrado por parte de las organizaciones tanto en sus comunicaciones como en la información almacenada en equipos y dispositivos.

10.2 Grupo de Tendencias II: Código Dañino

TENDENCIA II.1: La detección y eliminación del código dañino avanzado consumirá más tiempo

Todos los indicios que hemos visto en 2013 hacen sospechar que la detección del código dañino avanzado absorberá más tiempo que lo hace ahora. Dependiendo de las fuentes consultadas[152], la detección de una violación sofisticada puede consumir entre 80 y 100 días, y su solución entre 120 y 150 días. Es muy posible que estos tiempos aumenten en 2014. Análogamente, los tiempos de limpieza también se incrementarán, especialmente en ataques complejos que, una vez comprometida una organización, pueden mantenerse por largos periodos de tiempo sin ser descubiertos y que disponen de puertas traseras que se activan cuando han confirmado la detección y limpieza del primer ataque.

TENDENCIA II.2: La disminución del volumen del código dañino avanzado

La cantidad de nuevo código dañino está comenzando a disminuir[153]. Es de esperar que los ataques sean más precisos lo que permitirá usar menores cantidades de código dañino para acceder a las credenciales de los usuarios e iniciar su infiltración por las redes comprometidas. Así, aunque el número de ataques disminuya, el riesgo puede ser mayor, debido a la complejidad de los mismos.

150 Por ejemplo, en octubre de 2013, los investigadores del Websense Security Labs descubrieron un perfil falso en LinkedIn que identificaba objetivos para una inminente campaña de phishing. Un falso usuario llamado "Jessica Reinsch" contactó con usuarios concretos de LinkedIn, elegidos específicamente por ocupar un determinado puesto de trabajo en organizaciones de características concretas. Los atacantes instaron a tales contactos a visitar su sitio web dañino. (http://community.websense.com/blogs/securitylabs/archive/2013/10/31/linkedin-lure-looking-for-love-ly-profiles-possibly-more.aspx)

151 Según Symantec (2014 Predictions).

152 Verizon Data Breach Investigations Report , Ponemon Institute y otros.

153 Fuente: Websense ThreatSeeker ® Cloud Intelligence Cloud.

Por otro lado, si los atacantes son capaces de sustraer las credenciales de algún usuario corporativo, podrían acceder a los servicios en la nube y a la infraestructura móvil de la organización (por ejemplo, VPN ó RDP). Este acceso posibilitaría a los atacantes alcanzar su objetivo sin recurrir a la distribución masiva del código dañino.

TENDENCIA II.3: El *ransomware* atacará a las organizaciones

Websense señala que, en 2014, las organizaciones deberán redoblar sus esfuerzos para mitigar ataques que, en algunos casos, pretenderán la destrucción de los datos corporativos.

El ransomware[154] se empleará en atacar organizaciones pequeñas y medianas. De hecho, en 2013, el resurgimiento de CryptoLocker, demostró cómo una pequeña pieza de código dañino, en un único equipo, podía mantener como rehén a toda una organización.

Los beneficios económicos del ransomware puedan ser muy significativos. Además, en muchas ocasiones, no se liberarán las máquinas infectadas tras haber satisfecho el rescate.

TENDENCIA II.4: Muchas botnets migrarán de los tradicionales Servidores de Mando y Control (C&C) a redes *Peer-to-Peer* (P2P)

Las botnets tradicionales suelen utilizar el modo cliente-servidor para comunicarse con el servidor externo de Mando y Control (C&C). Cuando se detecta un servidor y se desactiva, se dificulta al atacante volver a tomar el control de las máquinas comprometidas. Utilizando P2P esta situación cambia drásticamente. Cada PC en una red P2P podría desempeñar la función de servidor o cliente, con lo que la botnet resulta más difícil de desactivar. Algunas de las principales botnets que han migrado a este nuevo modelo han sido **ZeroAccess, Kelihos, Bublik y Zeus v3**. Durante 2014 crecerá esta técnica de persistencia.

10.3 Grupo de Tendencias III: Dispositivos Móviles

TENDENCIA III.1: El código dañino para Android, los Sistemas de Control Industrial y la Internet de las Cosas

Durante los últimos años, el número de líneas que conectan máquinas entre sí (M2M), ha crecido continuamente y, durante julio de 2013, se superó la barrera de los tres millones de líneas (según el Informe de Telefónica ya citado). Y aunque esta cantidad viene a suponer tan sólo un 5,4% de los accesos móviles totales, su ritmo de crecimiento es del 12,5%.

Así las cosas, los desarrolladores de aplicaciones para Android pondrán el foco en encontrar mercados sin explotar para este sistema operativo. Algunos de estos mercados emergentes incluirán, además de todo tipo de dispositivos portátiles (tabletas, consolas portátiles para juegos, los denominados Warables[155], etc.), equipos y dispositivos de domótica, así como Sistemas de Control Industrial (ICS/SCADA)[156]. Es muy probable que en los próximos

154 Ramsonware. Código dañino que mantiene cifrados los datos personales / corporativos en tanto no se satisfaga un rescate.

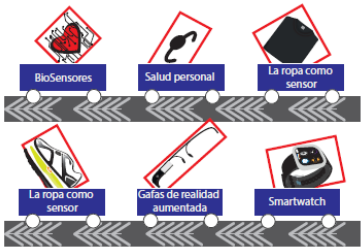
155 Dispositivos que el usuario lleva encima como si se tratara de complementos o ropa

156 Fortinet's FortiGuard Labs (Nov, 2013)

años aparezcan las primeras muestras del código dañino en estos nuevos tipos de dispositivos y sistemas.

En 2013 se han evidenciado ataques contra sistemas embebidos en televisores inteligentes, equipos médicos, cámaras de seguridad y monitores de bebé, entre otros, y aunque los principales proveedores de software disponen de mecanismos de notificación a los clientes y actualización, hay todavía muchas empresas que fabrican dispositivos cuyo software presenta graves problema de seguridad o no han previsto la forma de notificación a los usuarios, ni los mecanismos para parchear tal software. Es presumible que, en 2014, asistamos a renovadas amenazas en tal sentido.

Por otro lado, los ciberdelincuentes también podrán dirigirse a determinados dispositivos de automatización del hogar que puedan tener control sobre el consumo eléctrico, etc., al objeto de confirmar que alguien está o no en su casa en un momento dado.



10.4 Grupo de Tendencias IV: Los Servicios de Ciberseguridad

TENDENCIA IV.1: Los proveedores de sistemas de seguridad estarán obligados a ser más transparentes y a ofrecer productos y servicios certificados

En septiembre de 2013, la Comisión Federal de Comercio de los EE.UU. sancionó de manera importante a una empresa que comercializaba tecnología de monitorización de video para consumidores, por afirmar en sus folletos que su producto era "seguro", cuando la evidencia mostró claramente que no lo era. Durante 2014 los usuarios tenderán a exigir pruebas adicionales en relación con la seguridad de los productos o servicios que les son ofrecidos, lo que obligará a los proveedores a certificar sus productos o servicios conforme a Esquemas de Certificación de Seguridad[157] y, ser más transparentes en las características de tales servicios, los productos ofrecidos, la gestión de parches y el ciclo de vida del SW empleado.

157 En España, el Centro Criptológico Nacional (CCN) actúa como Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI), de aplicación a productos y Sistemas en su ámbito. (https://www.oc.ccn.cni.es/)

10.5 Grupo de Tendencias V: Exploits y Botnets

TENDENCIA V.1: La evolución de los exploits-kits

El exploit kit Blackhole ha sido, sin duda, el más destructivo de la historia (incorporaba con gran agilidad las vulnerabilidades más recientes). Arrestado su desarrollador, 2014 será testigo de una lucha por el liderazgo en el mercado de exploits-kits. A Blackhole le habían seguido en popularidad los exploits kits Cool, Gong da, **Neutrino y Redkit** . Para llena el vacío dejado, es presumible que los dos últimos alcancen una fuerte implantación en 2014[158].

TENDENCIA V.2: Los ataques cruzados de botnets

Históricamente, las botnets trabajaban de manera aislada, cuando una botnet como TDSL infectaba un ordenador, lo primero que hacía era eliminar cualquier otro malware de éste para evitar que el equipo infectado se volviera demasiado inestable. Con el tiempo, los creadores de botnets han ido siendo capaces de ocultar cada vez mejor su código dañino en los ordenadores infectados, lo que ha hecho que su detección por otras botnets fuera cada vez más difícil.

En la actualidad, en vez de competir por el control del equipo de la víctima, estamos asistiendo a una tendencia en la que varias botnets se alían en pos de **incrementar la base de usuarios infectados**. El primer ejemplo de esta cooperación se observó en 2009 con Virut. Durante 2013 hemos asistido a un incremento notable de esta actividad, con las botnets **Andromeda, Bublik, Dorkbot, Fareit y ZeroAccess**. En 2014 se incremente esta tendencia.

TENDENCIA V.3: Las repercusiones de los exploits Java de día-cero

Algunos expertos sostienen que, en 2014, los exploits Java zero-day podrían ser menos frecuentes. Se basan en que, a pesar de la relativa facilidad para desarrollar exploits Java, la aparición masiva de nuevos ataques Java de día-cero se ha detenido desde febrero de 2013, aunque las razones no están claras: puede ser debido en parte a las alertas de seguridad pop-up en Java 1.7 y a una mayor atención por parte de la comunidad de seguridad.

Sin embargo, otros analistas entienden que Java seguirá siendo altamente explotable y, en consecuencia, los sistemas desarrollados a su amparo, altamente explotados. Estos expertos afirman que a pesar de la publicidad que ha tenido este tipo de ataques en 2013, una buena parte de los usuarios finales siguen ejecutando versiones antiguas de Java y, por tanto, siguen estando extremadamente expuestos a los ataques.

10.6 Grupo de Tendencias VI: Ataques contra sistemas operativos y navegadores

TENDENCIA VI.1: Aumento de los ataques contra Windows XP

Microsoft finalizará el soporte para Windows XP el 8 de abril de 2014. Esto significa que las vulnerabilidades que se descubran no serán debidamente parcheadas, haciendo por tanto

158 Un dato: Neutrino ha incorporado rápidamente los exploit de día-cero de Microsoft Internet Explorer.

vulnerables todos los sistemas basados en XP. Según NetMarketShare[159], en septiembre de 2013 Windows XP seguía siendo utilizado por el **31,42% de los ordenadores** de todo mundo. De acuerdo con las estimaciones de Gartner, llegado el 8 de abril de 2014, más del 15% de las grandes organizaciones todavía estarán usando Windows XP en el 10% de sus ordenadores. Por todo ello, es presumible que en 2014 se desarrollen exploits día-cero y se esperen al 8 de abril para venderlos al mejor postor. Estos exploits se usarán para lanzar ataques complejos contra empresas y organizaciones.

TENDENCIA VI.2: Las vulnerabilidades en los navegadores podrán ser más frecuentes

Los atacantes son cada vez más capaces de eludir el mecanismo ASLR (Address Space Layout Randomization) de los navegadores y, en contraste con el ritmo de desaceleración de las vulnerabilidades zero-day de Java, aquellas que involucran a los navegadores se incrementarán previsiblemente en 2014.

TENDENCIA VI.3: La evasión de de los sistemas automáticos de análisis

En 2014 es presumible que los atacantes estén en condiciones de encontrar nuevas formas de eludir los sistemas automatizados de análisis (sandbox). Un ejemplo: el código dañino que se activa a una hora específica, con ataques similares a los que se han visto en 2013 en Japón y Corea.

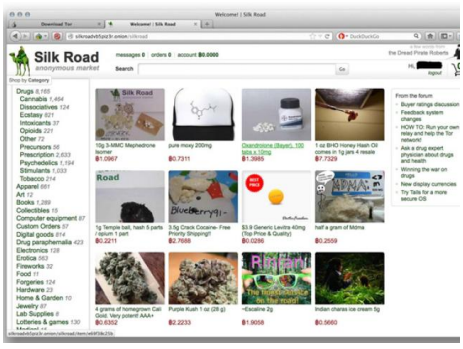
TENDENCIA VI.4: La destrucción de los sistemas operativos

En 2014 será testigo del incremento del código dañino que, como última fase de un ataque, destruirá los sistemas operativos de sus víctimas. Este es el caso de una de las nuevas características de Zeus, que elimina el sistema operativo, lo que ayuda a los atacantes a limpiar cualquier evidencia para dificultar la persecución del delito.

10.7 Grupo de Tendencias VII: Comportamientos Institucionales y Herramientas

TENDENCIA VII.1: El incremento de la cooperación entre las Agencias Nacionales de Ciberseguridad y los Cuerpos Policiales

2013 fue testigo de la actuación del FBI en cooperación con la NSA, haciendo caer la botnet de la llamada "Silk Road". La cooperación internacional de Agencias Nacionales de Ciberseguridad y Cuerpos Policiales ha cosechado importantes éxitos en 2013, como el caso de Dublín, donde, a principios de año, se desmanteló una de las redes más grande de tráfico de pornografía



159 http://www.netmarketshare.com/

infantil.

El cuadro de la figura siguiente muestran los precios de diferentes tipos de productos suministrados por la dark-net.

Site name	Address	Type of good	Cost	Normalized Cost (US$)
CloneCard	http://kpmp444tubeirwan.onion/board/int/src/1368387371226.jpg	EU/US credit cards	1 BTC	US$126
Mister V	http://wd5pbd4odd7jmm46.onion/	EU credit cards	€40–80	US$54–100
CC-Planet Fullz	http://tr36btffdmdmavbi.onion	EU/US credit cards	UA$40	US$54
CC 4 ALL	http://qhkt6cqo2dfs2llt.onion/	EU/US credit cards	€25–35	US$33–47
Cloned credit cards	http://mxdcyv6gjs3tvt5u.onion/products.html	EU/US credit cards	€40	US$54
NSD CC Store	http://4vq45ioqq5cx7u32.onion	EU/US credit cards	US$10	US$10
Carders Planet	http://wihwaoykcdzabadd.onion/	EU/US credit cards	US$60–150	US$60–150
HakPal	http://pcdyurvcdiz66qjo.onion/	PayPal accounts	1 BTC for US$1,000	US$126 for US$1,000
Onion identity	http://abbujjh5vqtq77wg.onion/	Fake IDs/passports	€1,000–1,150 (ID) €2,500–4,000 (passport)	US$1,352–1,555 (ID) US$3,380–5,400 (passport)
U.S. citizenship	http://ayjkg6ombrsahbx2.onion/silkroad/home	U.S. citizenship	US$10,000	US$10,000
U.S. fake driver's licenses	http://en35tuzqmn4lofbk.onion/	Fake U.S. driver's license	US$200	US$200
U.K. passports	http://vfqnd6mieccqyiit.onion/	U.K. passports	£2,500	US$4,000
Guttemberg prints	http://kpmp444tubeirwan.onion/board/int/src/1366833727802.jpg	Counterfeit money	1/2 of the monetary value	1/2 of the monetary value
High-quality Euro replicas	http://y3fpieiezy2sin4a.onion/	Counterfeit Euro banknotes	€500 for 2,500 CEUR €1,000 for 3,000 CEUR €1,900 for 6,000 CEUR	US$676 for 2,500 CEUR US$1,352 for 3,000 CEUR US$2,570 for 6,000 CEUR
Counterfeit U.S. dollars	http://qkj4drtgvpm7eecl.onion/	Counterfeit U.S. banknotes	US$600 for 2,500 CUSD US$2,000 for 5,000 CUSD	US$600 for 2,500 CUSD US$2,000 for 5,000 CUSD
Rent-a-Hacker	http://2ogmrlfzdthnwkez.onion/	Hacking services	€200–500	US$270–676
TOR Web developer	http://qizriixqwmeq4p5b.onion/	Web development	1 BTC per hour	US$126 per hour

Parece lógico pensar que en 2014 se incrementará la cooperación internacional de estos para actuar contra operadores mundiales de botnets y aquellas organizaciones o personas que prestan servicios o suministran herramientas a los ciberdelincuentes.

TENDENCIA VII.2: La Batalla por la "*Web profunda*"

En relación con la previsión anterior, es presumible que las Agencias Nacionales de Ciberseguridad de todo el mundo dirijan su atención en 2014 al desmantelamiento progresivo

de de la llamada Deep Web (sustentada muchas veces a través de Tor) y de ciertos servicios de intercambio de archivos muy cuestionados, del tipo de MegaUpload[160].

Es presumible que en 2014 asistamos a una renovada Silk Road.

TENDENCIA VII.3: La ciberseguridad ofensiva se hará pasar por "errores"

Durante años se ha venido hablando de ciberseguridad "ofensiva", como aquella actividad de ciberataques con la que gobiernos y empresas de todo el mundo podrían responder a quienes hubieren atacado previamente sus intereses. Al igual que lo que sucede en la guerra tradicional, los "errores tácticos" harán su aparición en algún momento.

Aunque se puedan justificar los ciberataques en respuesta a ataques, la realidad es que atribuir correctamente la autoría de un ataque es extremadamente difícil, incluso para los más expertos. No identificar con precisión el autor podría desencadenar un ataque de represalia contra el propietario de un sitio web previamente comprometido por un ataque. Como resultado de todo ello, podríamos encontrarnos con organizaciones inocentes atrapadas en un fuego cruzado de ataques[161].

TENDENCIA VII.4: El incremento de la autenticación de dos factores

Es de esperar que 2014 sea testigo del incremento del uso de la autenticación de dos factores, además de diferentes formas de biometría para identificación. En 2013 Apple anunció que sus nuevos iPhone 5S integrarían autenticación de huellas digitales. No obstante, el dispositivo fue atacado unos días después de que el teléfono se pusiera a la venta.

10.8 Grupo de Tendencias VIII: Watering Hole y Cloud

TENDENCIA VIII.1: Se incrementarán los ataques por *Watering hole*[162] y el código dañino en la cadena de suministro

Los ataques utilizando mecanismos de Watering hole, así como el uso de las redes sociales, aprovechando ambos la supuesta neutralidad de su apariencia, podrían situarse en 2014 al nivel de las infecciones atribuidas a los correos electrónicos dirigidos.

TENDENCIA VIII.2: El código dañino en la cadena de suministro

Es de esperar que en 2014 la existencia de códigos dañinos en las actualizaciones de BIOS y firmware. Es especialmente relevante pues esta técnica de infección hace inútiles los procedimientos de limpieza utilizados actualmente.

160 La retirada del servicio de MegaUpload dio lugar al nacimiento de Mega, una plataforma más robusta que su antecesora.

161 Todo ello sin mencionar las enormes repercusiones legales (nacionales e internacionales) que tendría penetrar en esta dinámica.

162 En un ataque por Watering-hole, el actor, que quiere atacar a un grupo en particular (organización, sector o región), desarrolla las siguientes acciones: 1.Observa los sitios web que el grupo utiliza frecuentemente. 2. Infecta uno o varios de tales estos sitios web con código dañino. 3. Es bastante probable que algún miembro del grupo objetivo se infectará al acudir a tales sitios. Esta estrategia es muy eficiente, incluso con grupos que son resistentes al spear-phishing.

TENDENCIA VIII.3: El interés por los datos alojados en la nube

Se espera que, en 2014, se realicen ataques contra los datos almacenados en la nube, además de los situados en las redes corporativas[163]. Si los datos en la nube no están adecuadamente protegidos, podría ser más fácil –y más rentable- penetrar en la nube que en las redes corporativas. No debe olvidarse, en todo caso, que los ataques a las redes corporativas podrían ser un paso intermedio para alcanzar los sistemas cloud.

10.9 Grupo de Tendencias IX: El Hacktivismo

TENDENCIA IX.1: La evolución del hacktivismo

Durante 2014, es de esperar lo siguiente:

Atomización y compartimentación de células hacktivistas: Si se mantiene la pauta observada en 2013, las denominaciones y estructuras nacionales de Anonymous decaerán, cediendo paso a la emergencia de grupos pequeños y compartimentados, con identidades propias, aunque empleando la misma iconografía o narrativa, pero que se definen primordialmente como hacktivistas sin circunscribirse a Anonymous. Estas células operarán, desde una narrativa anticapitalista y antisistema, con capacidad de comprometer la estética (defaces) o la información (exfiltraciones) de las páginas webs de instituciones públicas o empresas.

Incremento de intersección entre activismo y hacktivismo: Las células hacktivistas se aproximarán a grupos los activistas del mundo físico, principalmente aquellos que tengan narrativas militantes menos filosóficas o generalistas (menos políticamente elaboradas) y más concentradas en reivindicaciones sobre aspectos concretos de la ciudadanía (desahucios, rentas, suministros básicos, transporte, etc.). La implicación de células hacktivistas con colectivos de activistas físicos no tendrá sólo la forma de ciberataques, sino que comprenderá el diseño y construcción de medios de comunicación seguros para activistas, medios online para campañas en redes sociales y cibertácticas especialmente dedicadas a erosionar la reputación corporativa de gobiernos y corporaciones.

Probable empleo del hoax como táctica hacktivista: Determinados escenarios de 2013 sugieren que grupos hacktivistas, en combinación o no con colectivos activistas, podrían realizar convocatorias de ciberataque en el plano virtual o de manifestación de protesta en el plano físico, con la intención de movilizar una respuesta de los servicios de seguridad, sin que finalmente se produzca ningún ciberataque o protesta física.

Empleo por parte de gobiernos de la retórica hacktivista para conseguir sus propios objetivos.

163 Tales como Google, Microsoft Office 365 y Confluence.