CCN-CERT IA-09/15

CIBERAMENAZAS 2014 TENDENCIAS 2015

Resumen Ejecutivo

XX de xxxxxx de 2015

CONTENIDO

1 | PRÓLOGO

Si algo ha caracterizado al año 2014 ha sido la especial virulencia en los ataques contra la seguridad de los sistemas de las Tecnologías de la Información y las Comunicaciones (TIC) de gobiernos, administraciones públicas y empresas con alto valor estratégico. Los incidentes de gran envergadura se han venido sucediendo, mes a mes, en un intento continuo, por parte de los atacantes, de apropiarse de información valiosa o sensible desde los puntos de vista político, estratégico, de seguridad o económico. Es lo que hemos venido denominando como acciones de **ciberespionaje**.

También la **ciberdelincuencia**, con nuevos modelos de negocio como el Crimen como Servicio; el **hacktivismo**, con intenciones más modestas, pero que también pueden poner en peligro la prestación de servicios y el normal funcionamiento de las organizaciones; o el **ciberterrorismo** y la **ciberguerra**, como potenciales amenazas, han hecho acto de presencia en un año en el que **España** no ha sido ajena, ni mucho menos, en este mapa de ciberataques de todo tipo. Por el contrario, nuestro país **ha sido uno de los más castigados** por las ciberamenazas, especialmente en materia de ciberespionaje y ciberdelincuencia organizada.

España ha sido uno de los más castigados por las ciberamenazas, especialmente en materia de ciberespionaje y ciberdelincuencia organizada

Adentrarse en este panorama, sus orígenes, desarrollo y consecuencias e, incluso, vislumbrar las **tendencias** para los próximos meses en materia de ciberseguridad son los objetivos del ***Informe de Ciberamenazas 2014 y Tendencias 2015*** (CCN-CERT IA-9/15) que, por séptimo año consecutivo, ha elaborado el **CCN-CERT**, del **Centro Criptológico Nacional (CCN)**, dependiente del **Centro Nacional de Inteligencia** (CNI).

Su elaboración es el resultado de la experiencia del CERT Gubernamental Nacional, cuyas competencias son la gestión de ciberincidentes que afecten a **sistemas clasificados**, de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Se han utilizado, además, otras fuentes documentales, nacionales e internacionales, públicas y privadas.

Este documento contiene un **análisis, nacional e internacional**, de las ciberamenazas y de su evolución, así como cinco anexos de gran interés:

- Actividad del CCN-CERT
- Dispositivos móviles: ciberamenazas y tendencias
- Hacktivismo
- Campañas de ciberespionaje (Informe independiente: CCN-CERT IA-10/2015. *Clasificación: Difusión Limitada)*
- Recopilación de noticias e incidentes de seguridad más significativos de 2014.

La profusión de los datos recogidos (agentes de la amenaza, herramientas utilizadas para realizar los ciberataques, vulnerabilidades, medidas, tipología de ciberincidentes y campañas más destacadas o las ciberamenazas en dispositivos y comunicaciones móviles) da como resultado un informe de más de 160 páginas (disponible en la parte privada del portal www.ccn-cert.cni.es), cuyo Resumen Ejecutivo presentamos en este documento.

2 AGENTES DE LA AMENAZA

¿Quiénes?

El Informe CCN-CERT IA-09/15 realiza un exhaustivo análisis de los agentes de la amenaza, su origen, motivaciones, así como las técnicas y capacidades que han evidenciado.

2.1 Estados: Ciberespionaje

El CCN-CERT gestionó 12.916 incidentes, de los cuales, 132 fueron catalogados como críticos

La amenaza del **ciberespionaje** originado en los propios estados o por las empresas ha alcanzado, durante 2014, la **máxima intensidad** conocida hasta la fecha y ha supuesto, sin duda, la mayor amenaza para la ciberseguridad de los intereses nacionales. Se ha sido testigo del incremento del número de casos registrados y de la complejidad e impacto de sus acciones, lo que ha provocado la necesidad de potenciar las capacidades de detección, análisis y respuesta de los servicios públicos competentes en todo el mundo, muy especialmente los Servicios de Inteligencia.

Este ciberespionaje ha fundamentado sus acciones en el uso de **técnicas APT** *(Advanced Persistent Threat),* dirigiéndose contra distintos objetivos que, en el caso de España, se han centrado en determinados departamentos de las administraciones públicas españolas, la industria de la Defensa, aeroespacial, energética, farmacéutica, química, TIC, asi como los dispositivos móviles del personal directivo de estos sectores.

De hecho, este tipo de ataque está detrás de los incidentes con mayor peligrosidad de los gestionados por el CCN-CERT. En total, en 2014, el CERT Gubernamental Nacional abordó 12.916 incidentes, de los cuales, 132 fueron catalogados como críticos; es decir, aquellos que pueden causar degradación de los servicios para un gran número de usuarios, implicar una grave violación de la seguridad de la información, pueden afectar a la integridad física de las personas, causar importantes pérdidas económicas, ocasionar daños irreversibles a los recursos de la organización, se puede incurrir en delitos y/o sanciones reglamentarias u ocasionar un daño muy grave en la imagen de la organización.

Sin mencionar el origen concreto de este tipo de amenzas *(el Informe CCN-CERT IA-10/15 de Difusión Limitada recoge un resumen de las principales campañas de ciberspionaje),* no hay que olvidar que los estados también pueden desarrollar sus ataques contratando servicios de otros actores (y operando, en consecuencia, bajo otra bandera) o haciéndose pasar por movimientos hacktivistas.

2.2 Ciberdelincuencia

El año 2014 ha demostrado que la delincuencia en el ciberespacio se está organizando de manera más profesional, usando Internet para la perpetración de múltiples tipos de delitos y con el objetivo final del beneficio económico. Algunas de sus formas de actuación más destacadas:

- Ciberataques del tipo **denegación de servicio distrituido (DDoS) o**

El ransomware y, en concreto, su versión más agresiva, el cryptoware, ha ido en aumento y sofisticación

introducción de código dañino en los sistemas de información de las víctimas, como forma de chantaje. El ***ransomware***[1] (más innovador y agresivo durante 2014 que nunca) y, en concreto, la aparición del llamado ***cryptoware,*** ha ido en aumento y sofisticación en los medios de pago de los rescates (a través de tickets o de moneda digital, como el Bitcoin). El CCN-CERT ha detectado más de 200 incidentes de este tipo en las Administraciones Públicas.

- ***Crimen como Servicio*** *(Crime-as-a-Service)* en los que terceras partes desarrollan los ciberataques. Este modelo ha crecido en tamaño, complejidad y profesionalidad. Se ha observado también que los precios para el despliegue de botnets y DDoS están disminuyendo gracias a la aparición de otras opciones. En contraposición a lo anterior, el precio de vulnerabilidades nuevas ha crecido significativamente.
- Comercio de servicios o de información robada mediante **botnets**[2] o código dañino.
- Uso del ciberespacio para desarrollar otras formas de delito al descubrirse la contratación de servicios de determinados hackers por parte de organizaciones del narcotráfico.

2.3 Hacktivistas

Hacktivistas: Personas o grupos, más o menos organizados, cuyas prácticas persiguen el control de redes o sistemas para promover su causa o defender sus posicionamientos políticos o sociales, basados en motivos ideológicos. En los últimos años sus ciberataques (desfiguración de páginas web, ataques DDoS, etc.) pretendían ser respuesta contra determinadas medidas adoptadas por distintos gobiernos. Sus conocimientos y capacidades varían mucho de un grupo a otro.

En el plano internacional han destacado los focos hacktivistas paralelos a conflictos sociales o políticos (Israel, Ucrania, Hong Kong, Turquía, Pakistán), así como la actividad individual de varias entidades hacktivistas como el 'Syrian Electronic Army', 'Anonymous Italia' o 'Lizard Squad'.

[1] *Consiste en el secuestro del ordenador (imposibilidad de usarlo) o el cifrado de sus archivos (Cryptoware) y la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.*

[2] *Una botnet es una red de ordenadores infectados que se emplean para actividades ilegales, por ejemplo, para lanzar a su través ataques de denegación de servicio distribuido (DDoS) contra un sistema concreto.*

En España ha decaído la presencia hacktivista de entidades locales, manteniéndose *'La 9ª Compañía'* como único referente operativo. En cambio, se ha observado un incremento leve de ataques de entidades hacktvistas marroquíes contra páginas web de bajo nivel localizadas en nuestro país.

El **Anexo C** del Informe completo de Amenazas CCN-CERT IA-09/15 contiene un Informe monográfico sobre la ***«Amenaza hacktivista en 2014»***.

2.4 Terrorismo

Los grupos terroristas todavía no han alcanzado las habilidades precisas o no han tenido acceso a los medios para desarrollar ataques complejos. En todo caso, grupos yihadistas han ejecutado ciberataques a pequeña escala (esencialmente, desfiguraciones de páginas web y ataques DDoS) en diferentes lugares, generalmente en respuesta a pretendidas hostilidades contra intereses islámicos.

Más frecuente es la utilización de Internet con fines de financiación, coordinación, propaganda, reclutamiento y radicalización.

Sea como fuere, el conocimiento que vienen adquiriendo los grupos terroristas podría tener en el futuro enorme importancia, razón por la cual es necesario adoptar una actitud de permanente vigilancia sobre tales extremos.

2.5 Otros actores

2.5.1 *Cibervándalos* y script *kiddies*

Cibervándalos: aquellos individuos que, poseyendo significativos conocimientos técnicos, llevan a cabo sus acciones con el único motivo de demostrar públicamente que son capaces de hacerlo.

Script kiddies: aquellos que, con conocimientos limitados y haciendo

uso de herramientas construidas por terceros, perpetran sus acciones a modo de desafío, sin ser, en muchas ocasiones, plenamente conscientes de sus consecuencias.

En 2014, las acciones imputables a ambos tipos de ciberdelincuentes no han mostrado significativos cambios respecto de años anteriores.

2.5.2 Actores internos

O insiders, aquellas personas que tienen o han tenido algún tipo de relación con una organización, incluyendo exempleados, personal temporal o proveedores.

Pueden constituir una de las mayores amenazas y su motivación suele ser siempre similar: venganza, motivos financieros o políticos, etc.

Además, es preciso tener en cuenta que estos actores pueden ser empleados por cualquiera de los cuatro primeros (especialmente por el ciberespionaje) para la infección preliminar de la red objetivo o para la exfiltración de información de la misma.

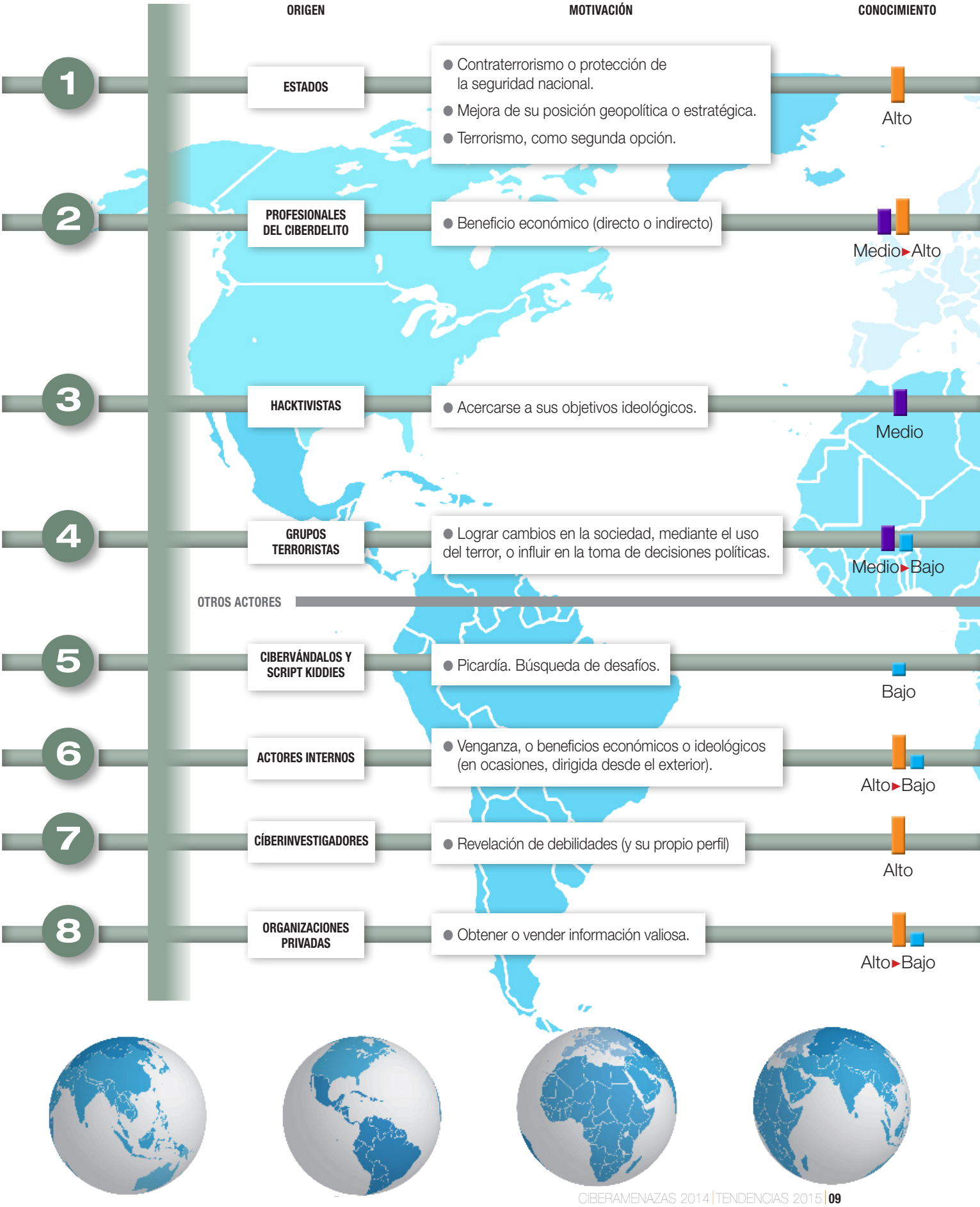
2.5.3 *Ciberinvestigadores*

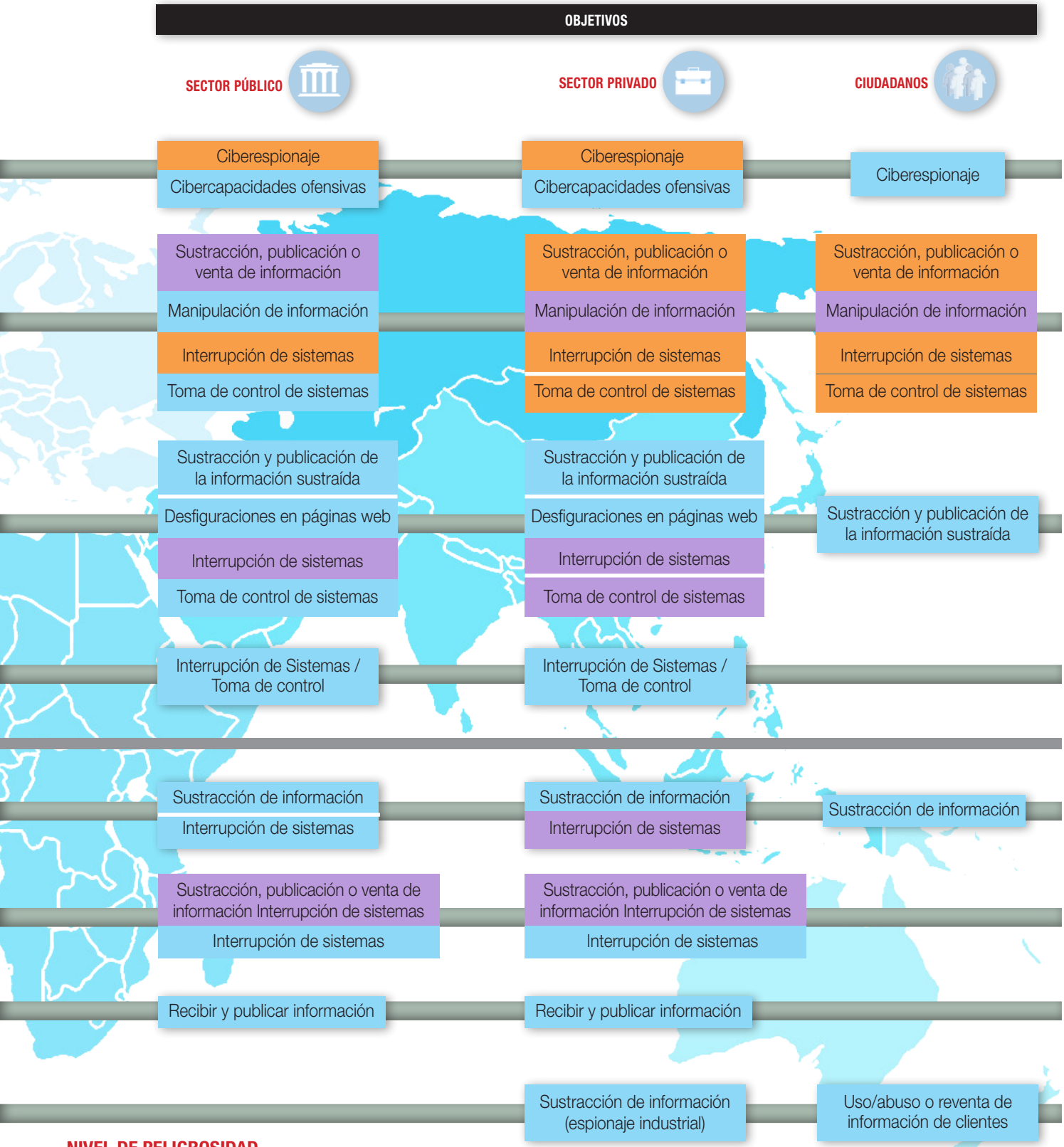
Aquellas personas que persiguen el descubrimiento de las vulnerabilidades que pueden afectar a los sistemas (hardware o software). La publicación de los resultados de sus investigaciones puede suponer que sus revelaciones se usen por terceros malintencionados.

2.5.4 Las organizaciones privadas

Las motivaciones para perpetrar ciberataques también se encuentran en Organizaciones privadas cuando, movidas por el interés económico que supone poseer los conocimientos que tiene la competencia, desarrollan acciones de ciberespionaje industrial.

AGENTES DE LA AMENAZA





NIVEL DE PELIGROSIDAD

BAJO

- No se han observado nuevas amenazas o tendencias, o
- Se dispone de medidas suficientes para neutralizar la amenaza, o
- No ha habido incidentes especialmente significativos en el periodo analizado.

MEDIO

- No se han observado nuevas amenazas o tendencias, o
- Se dispone de medidas (parciales) para neutralizar la amenaza, o
- Los incidentes detectados no han sido especialmente significativos.

ALTO

- Las amenzas o su tendencia se ha incrementado significativamente.
- Las medidas adoptadas tienen un efecto muy limitado, por lo que la amenaza permanece.
- Los incidentes detectados han sido especialmente significativos.

3 HERRAMIENTAS Y MÉTODOS DE ATAQUE

¿Cómo?

Durante 2014, los atacantes han hecho uso de herramientas y métodos de ataque nuevos (aparte de los tradicionales), más efectivos y rentables.

En general han sido más efectivas y rentables, como lo demuestra la existencia de las nuevas botnets que se han utilizado para los ataques DDoS más relevantes.

El spear-phishing[3] ha seguido constituyendo el elemento más utilizado para propagar este tipo de infecciones.

Por su parte, el denominado ransomware ha sido más innovador y agresivo. Quizás, el ejemplo más significativo lo encontramos en las infecciones por cryptoware, que ha supuesto para las organizaciones delincuenciales un nuevo y lucrativo modelo de negocio.

Todo ello ha dado lugar al desarrollo del denominado *Crime-as-a-service,* capaz de hacer posible ataques a gran escala por parte de usuarios con pocos conocimientos técnicos.

3.1 *Exploits*[4]

Su número ha disminuido en 2014 (situándose en torno a mil al año), aunque el precio en el mercado de tales herramientas (especialmente, de los llamados exploits de día-cero) ha crecido al mismo ritmo. Esta circunstancia ha venido provocando el desarrollo de un mercado negro de exploits capaz de mover anualmente enormes sumas de dinero.

PLATAFORMA	PRECIO*
Adobe Reader	5.000 – 30.000 $
Mac Os X	20.000 – 50.000 $
Android	30.000 – 60.000 $
Plug-ins navegadores Flash o Java	40.000 – 100.000 $
Microsoft Word	50.000 – 100.000 $
Microsoft Windows	60.000 – 120.000 $
Firefox o Safari	60.000 – 150.000 $
Chrome o Internet Explorer	80.000 – 200.000 $
Apple iOS	100.000 – 250.000 $

Exploit de Día Cero. Fuente: FORBES

3.2 Código dañino

Cuatro son su características principales:

- Complejidad: desde los virus de 1997 hasta el ransomware actual, las herramientas de APT o la utilización de las infraestructuras Web (DNS[5]).
- Su incremento constante en número (alcanzado los 25 millones de muestras).

[3] *Consiste en una estafa en forma de correo electrónico dirigido específicamente al objetivo para conseguir datos personales que puedan ser utilizados posteriormente en beneficio del atacante.*

[4] *Un* exploit *es un programa que explota o aprovecha una vulnerabilidad de un sistema informático en beneficio propio. Por su parte, los llamados* exploit *de día-cero* (zero-day) *son aquellos que todavía no se han publicado y, por tanto, no disponen de soluciones de seguridad que eviten la vulnerabilidad.*

[5] *DNS (Domain Name System). Sistema de Nombre de Dominio, es un sistema que nombra a todos los equipos, servicios o recursos conectados otorgándoles una dirección.*

- Su capacidad de adaptación temporal (en muchas ocasiones, el malware constituye una variación de muestras precedentes).
- La mayor cantidad de código dañino corresponde con troyanos[6].

El Informe de Amenazas completo recoge numerosos datos sobre el malware: su volumen, tipología, distribución geográfica y por sector de actividad o métodos de infección.

Muestras de código dañino para Mac

2014 comenzó con cerca de 20 nuevas variantes únicas descubiertas en los primeros 2 meses.

Entre las nuevas variantes, 13 pertenecen a 5 nuevas familias. **Clientsnow**, se vió involucrada en la ejecución de ataques dirigidos.

Las 3 restantes nuevas familias –**Coinstealer**, **Cointhief** y **Laoshu**-afectaron a los usuarios normales de Mac.

Código dañino más publicitado en 2014

Muestras de código dañino para Pc

Downadup (Conficker) fue la mayor amenaza, especialmente en Oriente Medio, América del Sur y Asia.

Downadup y **Majava** fueron más detectados en Europa y América del Norte. Por su parte, **Sality** y **Ramnit** son también amenazas que han tenido impacto aunque en menor grado en las regiones mencionadas.

Los últimos en incorporarse fueron **Wormlink**, **BrowserExploit** y Expiro.

Asimismo, en 2014 se ha incrementado la detección de ransomware, con muestras de código dañino cada vez más innovadoras y agresivas, al tiempo que sofisticando el medio de pago de los rescates, a través de tickets o de moneda digital (cryptocurrencies), tal como Bitcoin. **España aparece entre los países especialmente atacados por este tipo de código dañino.**

[6] *Caballo de Troya o troyano, es un código dañino con apariencia de un programa inofensivo que al ejecutarlo brinda al atacante acceso remoto al equipo infectado, normalmente instalando una puerta trasera* (backdoor).

3.3 Código dañino para dispositivos móviles

Persigue los mismos objetivos que los que motivaron el desarrollo de malware para PCs (el Informe completo CCN-CERT 09/15, en su **Anexo B,** recoge un estudio en profundidad de ***«Dispositivos Móviles: Ciberamenazas y Tendencias»),*** aunque con algunas diferencias:

- Los fabricantes de los sistemas operativos para estos equipos (Apple, Google o Microsoft) mantienen el control de sus tiendas oficiales dónde se venden las aplicaciones. Por este motivo, el malware suele extenderse más lentamente, aunque una gran cantidad se difunde a través de las tiendas no-oficiales, foros o web. El llamado «jailbreak» o «rooteado»[7] del dispositivo incrementa significativamente el riesgo.
- Muchos servicios, especialmente la banca, suelen utilizar un segundo factor (canal) para la autenticación, por lo que hay tipos de código dañino que persiguen infectar al tiempo al PC y al equipo móvil.
- Existe código dañino que provoca llamadas o remisión de mensajes de texto a números de tarificación especial que pueden llegar a suponer importantes pérdidas económicas para la victima.

Como en años anteriores, Android sigue siendo el sistema operativo móvil más empleado y atacado, yendo por detrás iOS (Apple) y Windows Phone.Por otro lado, aunque existen fabricantes que lo consideran innecesario, muchas compañías de software antivirus vienen desarrolando productos para este tipo de dispositivos.

3.4 *Botnets* y *Spam*

Existe una creciente dificultad para detectar y erradicar las redes de robots (botnets), que se siguen utilizando para la diseminación de spam[8], para la ejecución de ataques DDoS, *spear-phishing*, *click-fraud*[9], *keylogging*[10], así como la difusión de ransomware o la sustracción de dinero digital.

---

[7] *El* Jailbreak *en Apple («fuga de la cárcel» o destrabar) o el* rooteado *en* Android *(acceso al directorio raíz) permite acceder por completo del sistema operativo del que se trate, con privilegios de administrador o* superusuario, *al suprimir algunas de las limitaciones impuestas por el fabricante.*

[8] *Correos, generalmente publicitarios enviados de forma masiva a miles de usuarios, también conocido como correo basura.*

[9] *O fraude del* «click» *es un tipo de fraude que se produce al marcar* (click) *sobre una publicidad en una página web que imita a un usuario legítimo.*

[10] *Registrador de pulsaciones de teclado. Es un malware que captura los datos confidenciales como las contraseñas de usuario.*

Los datos de 2014 señalan un descenso en el número de botnets detectadas, aunque no su eficacia y su peligrosidad. De hecho, los atacantes ahora utilizan la red TOR[11] para ocultar botnets y/o servidores de mando y control (C&C),lo que dificulta enormemente su detección y erradicación.

3.5 Ataques *DDoS*

Tras unos años de relativa calma, los ataques DDoS regresaron con una intensidad inusitada. El ancho de banda usado y la duración de los ataques (muy prolongados, en ocasiones) dan fe de esta excepcional virulencia.

La razón de todo ello podemos encontrarla en la cada vez mayor sencillez para desarrollar ataques DDoS y la facilidad para acceder a determinadas herramientas (adquiridas en el mercado negro de la *hidden-wiki*[12], por ejemplo).

Una novedad de 2014 ha sido la aparición de ataques por amplificación DDoS por medio de protocolos UDP[13] y contra la infraestructura de red (ataques volumétricos).

También se han observado un incremento en los ataques dirigidos contra la capa de aplicación (capa 7), mucho más sofisticados y no necesariamente focalizados en el ancho de banda, que requieren un significativo nivel de conocimientos.

[11] *TOR (abreviatura de* The Onion Router*) es un software diseñado para permitir el acceso anónimo a Internet. Aunque durante muchos años ha sido utilizado principalmente por expertos y aficionados, el uso de la red TOR se ha disparado en los últimos tiempos, debido principalmente a los problemas de privacidad de Internet. Correlativamente, TOR se ha convertido en una herramienta muy útil para aquellos que, por cualquier razón, legal o ilegal, no desean estar sometidos a vigilancia o no desean revelar información confidencial.*

[12] *Es una enciclopedia que se encuentra alojada en la web oculta (*Hidden web *llamada también invisible web o deep web) y funciona como índice para acceder a páginas de dominio (.onion) que indica una dirección IP anómima accesible por medio de la red TOR (The Onion Route).*

[13] *UDP* (User Datagram Protocol) *es un tipo de protocolo de comunicaciones de nivel transporte, que no goza de las características de fiabilidad y seguridad, que el TCP (Transmision Control Portocol) pero en cambio es mucho más rápido; ideal para mensajes cortos, como en elsistema de nombres de dominio (DNS) o cuando no es relevante perder paquetes, como en el caso de transmisiones de audio o vídeo (stream).*

3.6 Phishing[14]

Como en años anteriores, el correo electrónico sigue siendo el medio preferido por los ciberatacantes para recabar información de las víctimas o para instarlas a descargar involuntariamente código dañino.

Se ha observado que la calidad de los mensajes de phishing ha mejorado notablemente, aunque lo más novedoso ha sido el uso combinado que del correo electrónico y del teléfono han empezado a hacer los atacantes (ingeniería social).

De igual forma, y como ya se ha señalado, el spear phishing ha sido el elemento más utilizado en este tipo de ataque. El atacante redacta el correo electrónico utilizando información de contexto de la víctima (obtenida en muchos casos de las redes sociales) para dar mayor verosimilitud e incluye un enlace con exploits-kits[15] o herramientas RAT[16]. Las garantías de éxito son, por tanto, muy elevadas.

3.7 Uso de certificados digitales

Creciente tendencia a utilizar certificados digitales (aparentemente legítimos) en el proceso de instalación de aplicaciones o como medio de autenticación.

Utilizando este procedimiento, los atacantes pretenden generar confianza a sus víctimas, haciéndoles creer que se trata de fuentes legítimas. La sustracción de certificados o la puesta en compromiso de Autoridades de Certificación suelen ser los medios elegidos para desarrollar este tipo de acciones, pudiéndose incluso diseminarse a través de redes de distribución automática de contenidos (CDN[17]) que confieren a los programas dañinos la apariencia de paquetes de software legítimos.

---

[14] *Suplantación de identidad. Consiste en el envío de correos electrónicos que aparentan ser fiables y que suelen derivar a páginas web falsas recabando datos confidenciales de las víctimas.*

[15] *Exploits-kits: Paquetes con programas dañinos.*

[16] Remote Administration *Tools, Herramientas de administración y acceso remoto.*

[17] Content Delivery Network.

4 VULNERABILIDADES

¿Dónde?

Como en años anteriores, las vulnerabilidades achacables al software siguen en niveles muy altos, mientras que las causadas por factores humanos y organizativos permanecen como uno de los eslabones de la cadena más débiles.

4.1 Vulnerabilidades técnicas

El caso Heartbleed, una vulnerabilidad en OpenSSL[18], aparecida en abril de 2014 y que permitía a los atacantes el acceso a la memoria de los equipos atacados, puso de manifiesto **la importancia de fomentar el desarrollo de software seguro, aún sabiendo que es imposible garantizar la construcción de programas y aplicaciones libres de errores.** En la siguiente tabla muestra las vulnerabilidades más destacadas de 2014[19]

IntelliShield ID	Vulnerabilidad	Urgencia	Credibilidad	Severidad
33695	OpenSSL TLS/DTLS HeartBeat Information Disclosure V.			
35880	GNU Bash Environment Variable Content Processing Arbitrary Code Execution V.			
35879	GNU Bash Environment Variable Function Definitions Processing Arbitrary Code Execution V.			
36121	Drupal Core SQL Injection V.			
32718	Adobe Flash Player Remote Code Execution V.			
33961	Microsoft Internet Explorer Deleted Memory Object Code Execution V.			
28462	Oracle Java SE Security Bypass Arbitrary Code Execution V.			
30128	Multiple Vendor Products Struts 2 Action: Parameter Processing Command Injection V.			

[18] *Biblioteca de programas que suele usarse por multitud de sistemas (servidores web, VPN, puntos de acceso WiFi, etc.) para el establecimiento de conexiones seguras. Al objeto de evitar un nuevo compromiso, las principales empresas tecnológicas anunciaron un amplio apoyo económico a OpenSSL y a otro software de código abierto. El caso Heartbleed dejó en el aire la posibilidad de que una problemática similar pudiera ocurrir con otro software de uso común.*

[19] Fuente: *CVSS. Common Vulnerability Scoring System.*

«Dispositivos y Comunicaciones Móviles: Ciberamenazas y Tendencias», Anexo B del Informe CCN-CERT IA-09/15

Aspectos destacados en el campo de las vulnerabilidades:

- Incremento en la explotación de las vulnerabilidades Java, Internet Explorer, Adobe Flash y Adobe Reader.
- **Actualización del software y fin de soporte:** en algunos dispositivos no es posible las actualizaciones de software, mientras que en otros sólo durante un tiempo limitado. Un ejemplo es el fin del soporte, el 8 de abril de 2014, de **Windows XP**[20], pese a que todavía hoy existe un gran número de usuarios con este sistema operativo.
- **Nuevas tendencias:** Ataques a Puntos de Venta o servicios en la nube.
- Empleo masivo de protocolos sin seguridad como BGP, DNS y SMTP[21] con escasas posibilidades de verificación, autenticación o cifrado, pese a ser esenciales en el enrutamiento del tráfico de Internet. Un ataque bien construido que explote las **vulnerabilidades de BGP** podría llegar a permitir monitorizar a gran escala el **tráfico de Internet,** con los riesgos que esto comportaría.
- **Dispositivos móviles:** La descarga de aplicaciones alcanzó los 80.000 millones. Normalmente estas no emplean adecuadamente los mecanismos de seguridad disponibles, realizan conexiones no autorizadas y recopilan información privada sin autorización expresa del usuario.

4.2 Factor humano y organizativo

Los nuevas tendencias orientadas a una mayor eficiencia en el negocio que implementan soluciones tipo BYOD[22] y el empleo de servicios externalizados y de almacenamiento en la nube (Cloud *Services*), las posibilidades que aporta el tratamiento masivo de datos (Big Data) **incrementan la superficie de exposición de las organizaciones** exigiendo la implementación de nuevas políticas y medidas de seguridad.

Por parte de los usuarios se destaca el empleo de contraseñas débiles y el uso masivo de redes sociales aportando información personal y corporativa que facilita el ataque.

[20] *CCN-CERT IA-02/14 Riesgos de* uso *de Windows XP* tras *el fin del* soporte.

[21] *BGP* (Border Gateway Protocol), *DNS* (Domain Name System), *SMTP* (Simple Mail Transfer Protocol).

[22] *CCN-CERT IA-21/13 Riesgos y Amenazas del BYOD* (Bring Your Own Device) *permite a los empleados a través de sus dispositivos móviles personales acceder a los servicios corporativos (correo principalmente).*

5 CIBERINCIDENTES

¿Qué?

Durante 2014 el número de *ciberincidentes* no ha dejado de aumentar y, lo que es más preocupante, su nivel de peligrosidad.

Existen diversas clasificaciones de la tipología de los incidentes (el CCN-CERT recoge la empleada por las AAPP en su ***Guía CCN-STIC 817 de Gestión de Ciberincidentes***) pero, en general, todas tienen en cuenta los ataques dirigidos a la información o a los sistemas.

5.1 Ataques dirigidos a la información

«Campañas de Ciberespionaje», Informe CCN-CERT IA-10/2015. Clasificación: Difusión Limitada

- ***Ciberespionaje:*** los ataques más importantes y peligrosos, sufridos por las instituciones y empresas de los países occidentales **–España, entre ellos–** (por ejemplo varios Ministros y Secretarios de Estado del Gobierno sufrieron diversas campañas de ataque dirigida contra los móviles y ordenadores personales de altos cargos del Ejecutivo, a través de un correo electrónico dañino).
- **Amenazas Persistentes Avanzadas *(APTs)*:** el informe CCN-CERT IA-10/15 recoge información sobre las acciones detectadas en 2014, su complejidad y sofisticación.
- **Robo o sustracción de información,** además de constituir el objetivo principal de las *APTs,* supone un tipo específico de amenaza que el informe estudia profusamente (*botnet Pony*[23], credenciales robadas, etc.)
- El **chantaje** como amenaza de publicación de determinada información.

5.2 Ataques dirigidos a las TIC

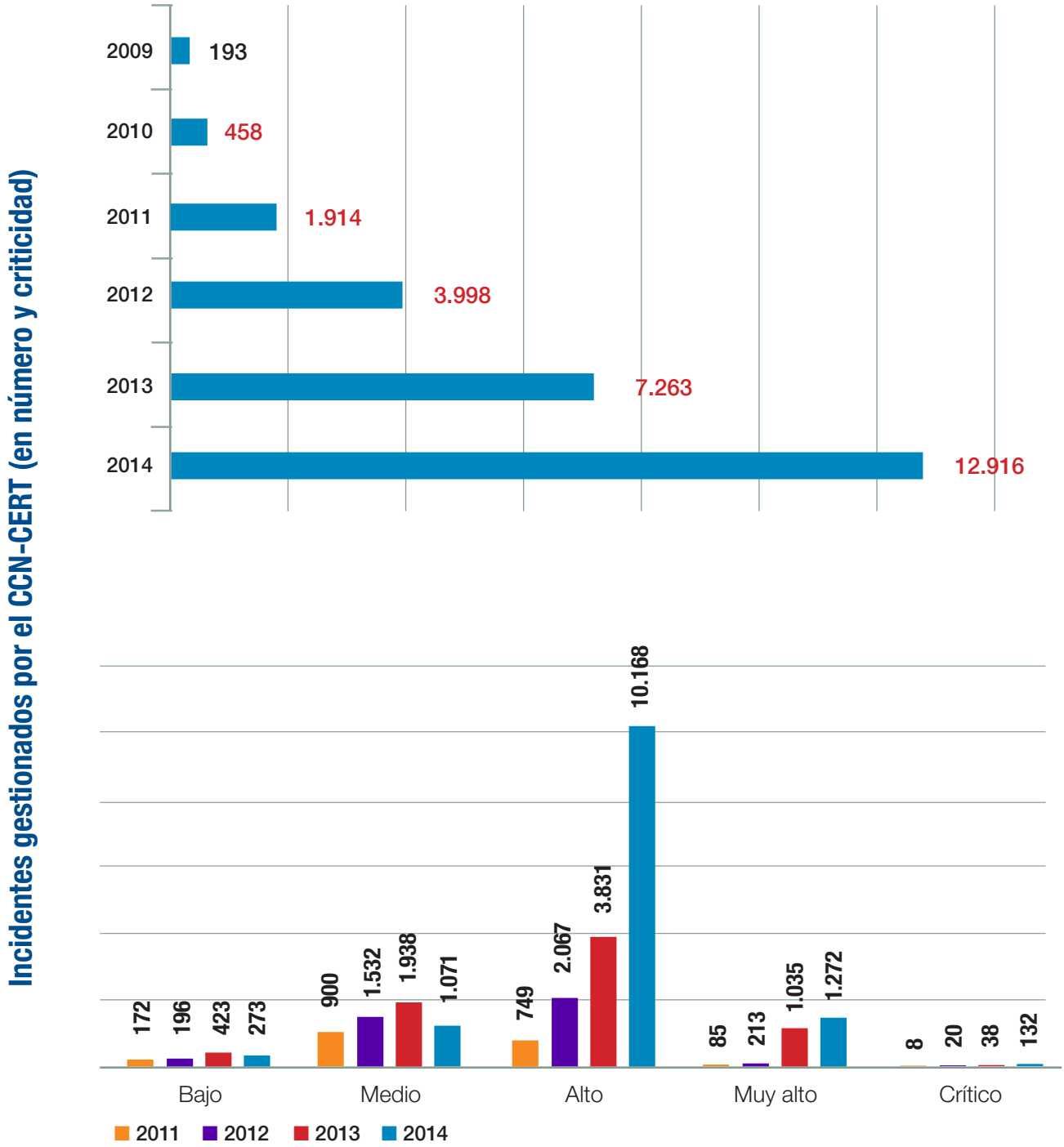
Además de la información que tratan o almacenan, en muchas ocasiones son los propios sistemas de información y las infraestructuras, los objetivos de los ciberataques. Entre ellos se encuentran:

- **Desfiguración:** los atacantes alteran el contenido de una página web, como los realizados por Anonymous y el Syrian Electronic Army (Informes CCN-CERT IA-01/14, IA-04/14, IA-08/14, IA-12/14 y IA-18/14 entre otros).
- **Interrupción y toma de control de infraestructuras:** empleo masivo por los atacantes de servicios web legítimos para usarlos como infraestructuras de mando y control así como puntos de salto para la extracción de información de las redes objetivo.
- **Servicios Cloud:** utilización de los servicios en nube como paso intermedio en la exfiltración de información de las redes atacadas.

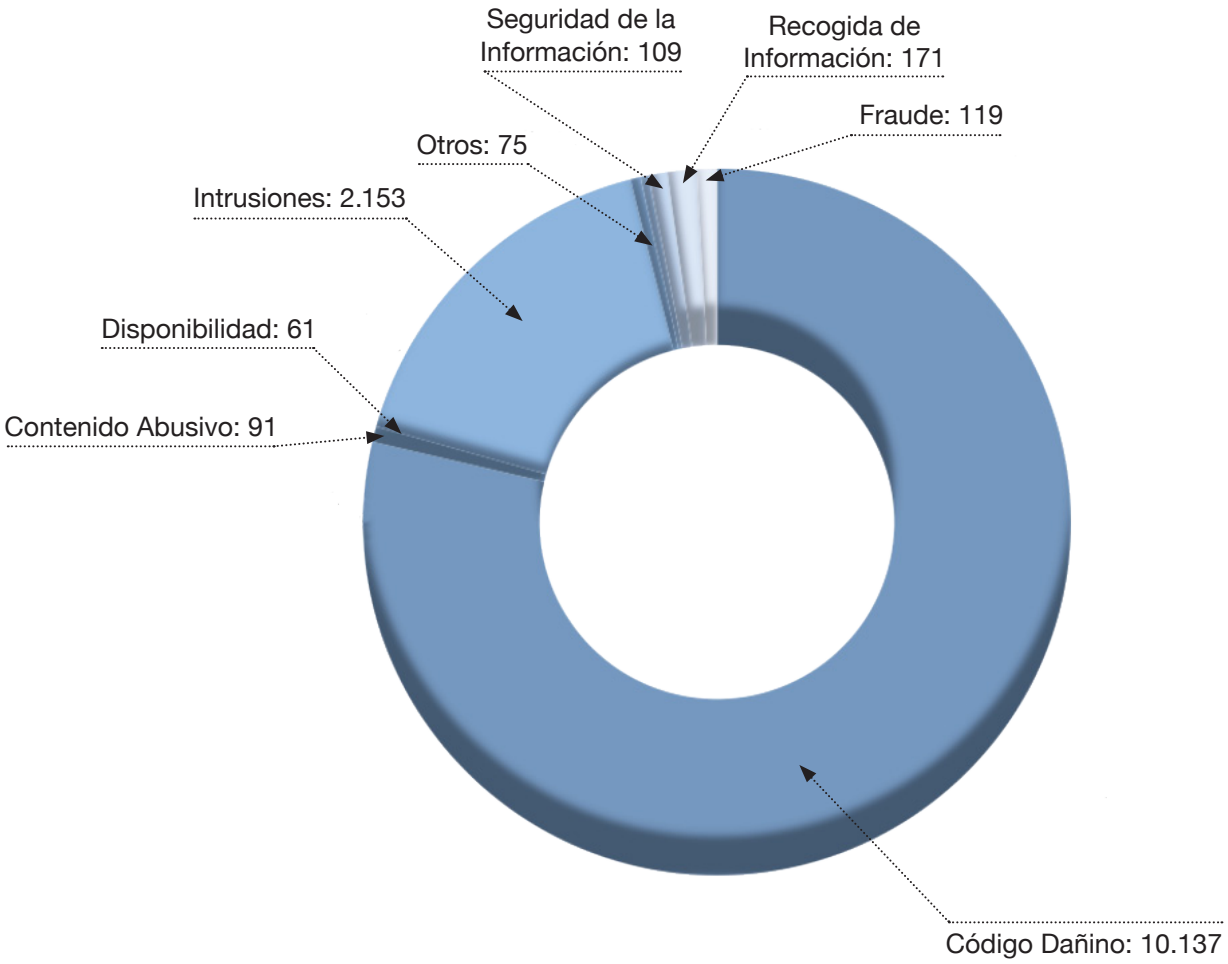
[23] *Se trata de una* botnet *que utiliza un tipo de malware del tipo* keylogger *(registrador de pulsaciones de teclado) que captura toda clase de información confidencial y datos de acceso a numerosas aplicaciones. Se denomina así al utilizar el logo del* pony *del famoso juego* «Farmville».

5.3 *Ciberincidentes* en España

Atendiendo los datos recabados por el CCN-CERT, 2014 ha sido un año especialmente significativo en materia de ciberamenazas, con especial importancia del ciberespionaje y APTs, código dañino y ransomware (el CERT Gubernamental Nacional publicó el Informe CCN-CERT IA-21/14 al respecto en diciembre).



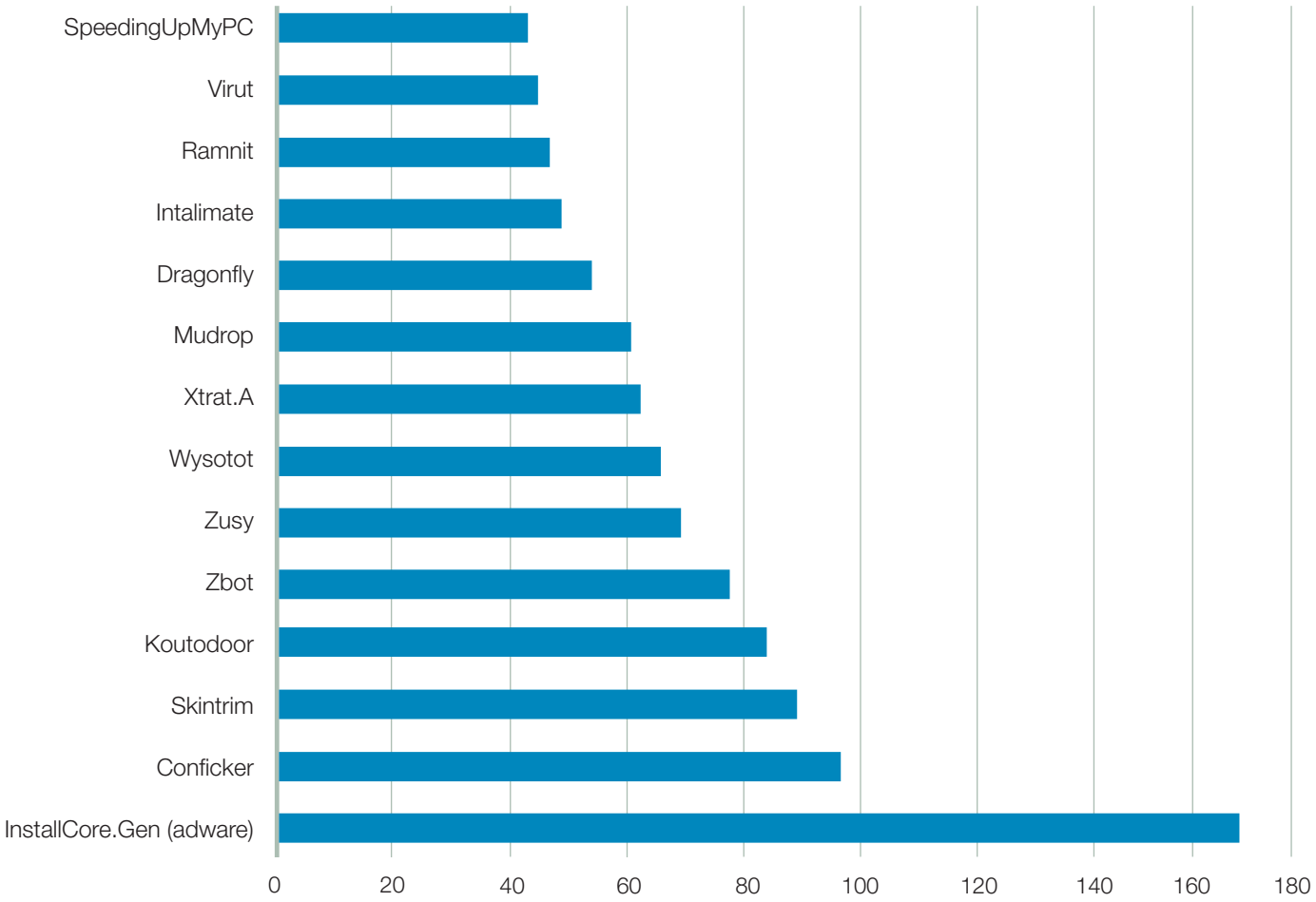
Principales subcategorías de incidentes gestionados en 2014



Principales subcategorías de incidentes gestionados en 2014

Subclasificación general	Clasificación	Nº incidentes
Troyano	Código Dañino	9.371
Explotación de vulnerabilidades	Intrusión	833
Inyección SQL	Intrusión	460
Inyección de Ficheros Remota	Intrusión	460
Gusano	Código Dañino	459
Spyware	Código Dañino	258

Código dañino más detectado por el CCN-CERT



6 MEDIDAS

¿Qué hacer?

Los esfuerzos se deben centrar en incrementar las capacidades de prevención, detección, análisis, respuesta y coordinación, unido a una política de investigación y de cambio en la mentalidad. Trabajar como si se estuviera comprometido y por lo tanto proteger los activos fundamentales en un medio comprometido.

En el caso de las AAPP, la aplicación de las medidas contempladas en el Esquema Nacional de Seguridad supone la mejor garantía

Algunas de las medidas necesarias son:

1. **Incremento de la capacidad de vigilancia:** Desplegar sistemas que potencien las capacidades de detección e investigación de incidentes en redes y sistemas, facilitando su contención y eliminación. Desplegar sistemas de gestión centralizada de eventos de seguridad y complementar con herramientas capaces de detectar anomalías de manera temprana.
2. **Intercambio de información de ciberamenazas:** Despliegue de sistemas que permitan el intercambio automático de reglas de detección e indicadores de compromiso para su integración en los sistemas de defensa.
3. **Protección frente a ciberataques de tipo DDoS:** Mediante la aplicación de configuraciones de seguridad[24] y servicios de filtrado de conexiones.
4. **Implantación segura de IPv6**[25]. Soporte a la migración a la nueva versión.
5. **Uso de medidas criptográficas,** incluyendo el uso de HTTPS[26], StartTLS[27] o el cifrado de las conexiones entre los centros de datos. *(Guía CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad).*
6. **Protección y vigilancia de servicios esenciales para la organización.** Tal y como señala el Esquema Nacional de Seguridad, el correo y los servicios web (o las denominadas sedes electrónicas en el caso de la Administración) son parte de estos servicios esenciales. En este sentido, en 2014, DNSSEC[28] se ha consolidado como un método especialmente útil para dotar de seguridad a los nombres de dominio. Usando DNSSEC, los visitantes de un sitio web pueden verificar si se encuentran realmente en tal sitio web o, por el contrario, han podido ser desviados a otra página web.
7. **Impulso de la I+D+i en ciberseguridad.** Mejora de las características de seguridad de los productos impulsando los correspondientes procesos de certificación. Desarrollo de nuevos proyectos que mejoren las capacidades de vigilancia e intercambio de información ágil para su empleo en los sistemas de detección.
8. **Sensibilización a todos los niveles:** directivos, empleados, profesionales y, ciudadanos.
9. **Formación en ciberseguridad.** Incremento en la formación y certificación de profesionales de ciberseguridad.
10. **Adecuación de la legislación:** el informe recoge un amplio capítulo de la normativa aparecida durante 2014 en todo el mundo y las distintas Estrategias de Ciberseguridad (incluida la española).

[24] *CCN-STIC 812 Seguridad en entornos y Aplicaciones Web y CCN-STIC 820 Guía de protección contra denegación de servicio.*

[25] *IPv6* (Internet Protocol Versión 6). *Aumenta el límite de direcciones de red admisibles, pasando de* 2^{32} *en el caso de la versión v4 a* 2^{128} *en la v6.*

[26] *HTTPS (Hypertext Transfer Protocol Secure). Protocolo de aplicación seguro de transferencia de hipertexto. Usa SSL/TLS (Secure Sockets Layer/Transport Layer Security) para crear un canal cifrado en comunicaciones entre el cliente y el servidor.*

[27] *STARTLS es una mejora del protocolo TLS que no necesita utilizar un puerto diferente para la comunicación cifrada.*

[28] *DNSSEC (Domain Name System Security Extensions). Extensiones de seguridad para el sistema de nombres de dominio, permitiendo la autenticación del origen de datos DNS.*

7 | TENDENCIAS 2015

¿Hacia dónde?

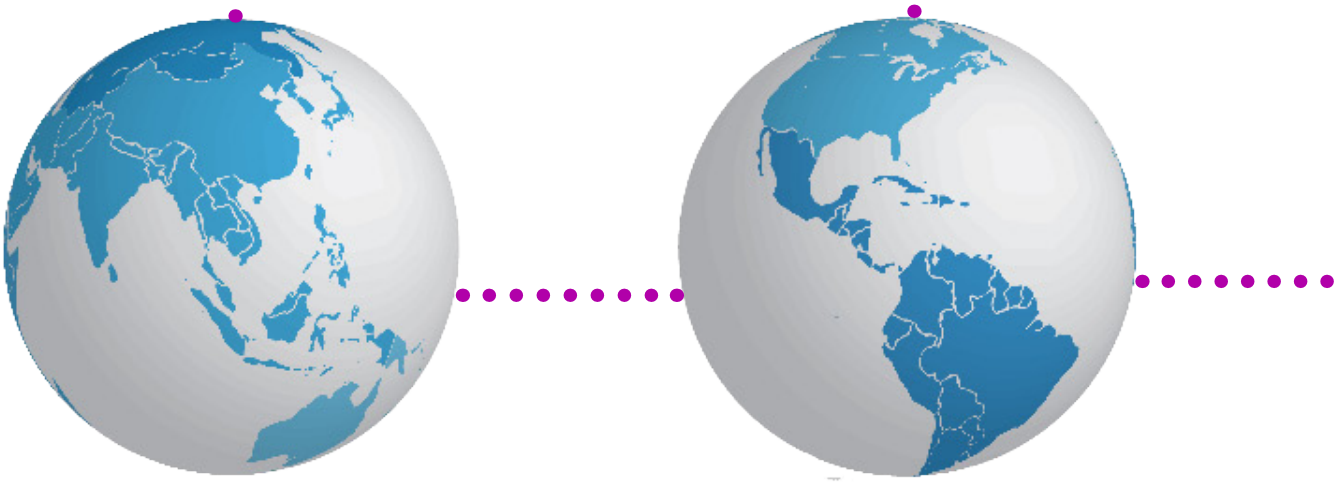
Las ciberamenazas siempre van por delante de las medidas que se adoptan. En este 2015, y en años futuros, se espera un incremento del ciberespionaje y el incremento de los ataques como servicio efectuados por grupos con conocimiento y capacidad técnica para realizarlos con garantías de éxito.

Atendiendo a lo señalado en los epígrafes anteriores, podemos esperar las siguientes tendencias para los próximos años:

PROBABILIDAD DE OCURRENCIA	AMENAZA
Ciberespionaje	El empleo del ciberespacio para la obtención de inteligencia se incrementará por todos los países de nuestro entorno por su eficacia y dificultad de atribución. Debido a la publicación de campañas de ciberespionaje realizada por compañías de seguridad, los países emplearán más recursos en la seguridad de sus operaciones aislando infraestructuras y diversificando las **Técnicas**, **Tácticas** y **Procedimientos (TTP)** de ataque.
Ataques como servicio	A través de grupos con conocimiento y capacidad técnica. Contratar sus servicios y planificar un ataque «a medida», con garantías de éxito. Requerirá ampliar el conocimiento de las redes Deep Web[29], incrementarse la cooperación público-privada y armonizar la legislación internacional.
Fusión de TTP utilizadas por el ciberespionaje y la ciberdelincuencia	Evolución de la actividad cibercriminal a TTP empleados en el ciberespionaje usando herramientas del tipo APT y dirigidas especialmente contra el sector financiero persiguiendo la sustracción de dinero.

PROBABILIDAD DE OCURRENCIA	AMENAZA
Herramientas de ataque para dispositivos móviles (principalmente ANDROID)	Se duplicará el número de amenazas a Android y las vulnerabilidades en los dispositivos móviles, plataformas y aplicaciones. Los datos comprometidos se usarán para otros ataques o para su venta en el mercado negro.
«Secuestro» de organizaciones por ransomware	Especialmente en sus variantes más agresivas, incluyendo grandes empresas e instituciones.
Incremento de ataques contra cajeros automáticos y procedimientos de pago	Se espera un incremento (y evolución) de los ataques contra estos dispositivos (y máquinas expendedoras de tickets), empleando técnicas APT para, a través de ellos, penetrar en la red de la entidad financiera. El uso de Windows XP[30] incrementa el riesgo.
Nuevas vulnerabilidades en software y protocolos habituales	A las peligrosas vulnerabilidades reveladas (Shellshock, Heartbleed y OpenSSL, etc.) se sumarán otras importantes.

■ MUY PROBABLE
■ PROBABLE
■ POSIBLE



PROBABILIDAD DE OCURRENCIA	AMENAZA
Ataques contra Infraestructuras Críticas	Muchos estados están preparándose para atacar los sistemas de control industrial (SCADA)[31] y otros sistemas críticos, como las redes de energía eléctrica.
Ataques contra Linux[32] y OS-X[33]	Fomentado por el incremento en su uso, la desactivación de determinadas medidas de seguridad por defecto (al objeto de permitir la instalación de software pirata) y el escaso desarrollo de herramientas de seguridad, dada la imagen de seguridad que tenían.
Ataques contra Internet of Things[34]	Su expansión llevará consigo un mayor debate sobre los problemas de seguridad y, especialmente, de privacidad derivados de su conexión. También se conocerán vulnerabilidades de los dispositivos que permitirán la inclusión de código dañino que monitorice la actividad de los usuarios.

MUY PROBABLE
PROBABLE
POSIBLE

[29] *Deep Web o Hidden Web es la web profunda u oculta, no accesible a través de navegadores convencionales. Usualmente, se utilizan herramientas como TOR (The Onion Router) para acceder a ella.*

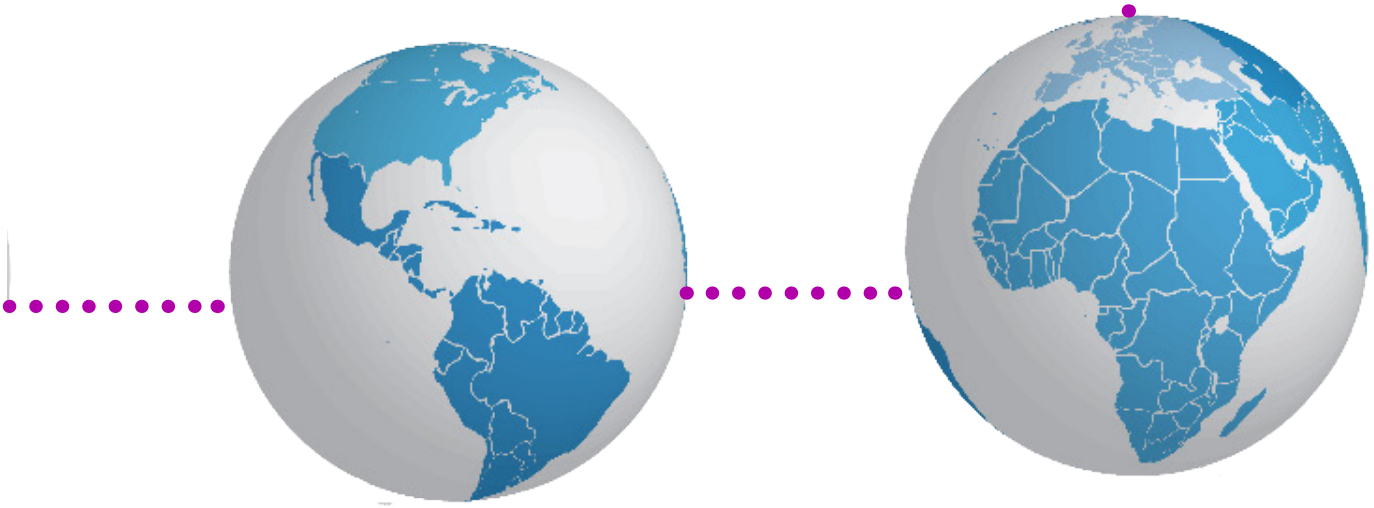
[30] *El 8 de abril de 2014, Microsoft dejó de dar soporte a Windows XP.*

[31] *SCADA (Supervisory Control And Data Adquisition). Software que permite controlar y supervisar procesos industriales a distancia.*

[32] *Linux: Sistema operativo de software libre, similar a Unix.*

[33] *OS-X (o Mac OS X): Sistema operativo basado en Unix y desarrollado por Apple Inc. Para dispositivos móviles existe una versión específica llamada iOS.*

[34] *Internet of Things: El Internet de las Cosas (IoT, por sus siglas en Inglés) referido a la interconexión de objetos cotidianos (dispositivos, sistemas y servicios) con Internet a través de redes fijas e inalámbricas y permitiendo al usuario un control y manejo de forma remota.*




www.ccn-cert.cni.es
www.ccn.cni.es
www.oc.ccn.cni.es
YouTube
CCN-CERT
centro criptológico nacional