CIBERAMENAZAS Y TENDENCIAS

EDICIÓN 2017

CCN-CERT IA-16/17

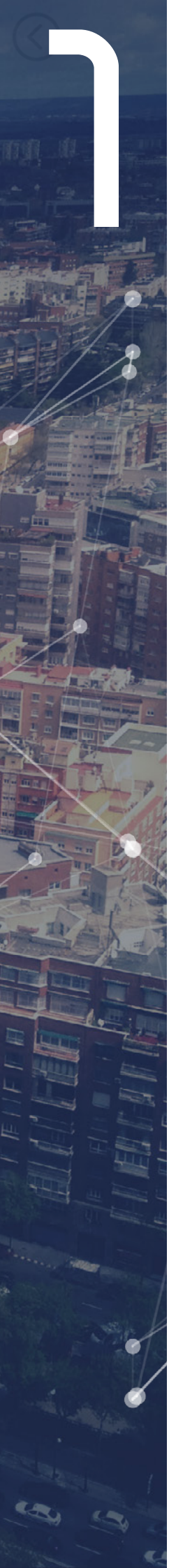
RESUMEN EJECUTIVO

ÍNDICE

PRÓLOGO	3
CIBERINCIDENTES	4
AGENTES DE LA AMENAZA	12
VULNERABILIDADES	15
MÉTODOS DE ATAQUE	18
MEDIDAS	23
TENDENCIAS	28

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2017.06.08 09:32:18 +02'00'



1 PRÓLOGO

El ciberespionaje, llevado a cabo habitualmente por servicios de inteligencia extranjeros, es donde reside la principal amenaza para el mundo occidental

La Capacidad de Respuesta de Ciberincidentes del Centro Criptológico Nacional (CCN-CERT) gestionó en el año 2016 un total de 20.940 **ciberincidentes**, detectados principalmente en el sector público y en empresas consideradas de interés estratégico para España, lo que supone un 14,5% más que en 2015. De ellos, el 3,6% fueron considerados por el equipo de expertos del CERT Gubernamental Nacional como muy altos o críticos, en función del grado de peligrosidad determinado por el tipo de amenaza, origen del atacante, perfil de la víctima, número o tipología de los sistemas afectados, impacto, inclusión o no en una campaña de mayor calado, etc.

Detrás de estas cifras, que no hacen sino crecer año tras año en nuestro país y en el resto del mundo, se encuentra información comprometida del más alto nivel; servidores bloqueados a la espera del pago de un rescate, desfiguraciones o denegaciones de servicio a diferentes páginas web; ataques a entidades financieras o interrupción de servicios energéticos.

Los ataques son perpetrados por distintos **Agentes de la Amenaza**, con diferentes **Métodos de Ataque**, aprovechando múltiples **Vulnerabilidades**, y para los cuales existen **Medidas** que hay que tener en cuenta para mejorar la protección.

A partir de diferentes fuentes y de la actividad diaria del Centro Criptológico Nacional (CCN), se desprende que es el ciberespionaje, llevado a cabo habitualmente por **servicios de inteligencia extranjeros**, donde reside la principal amenaza para el mundo occidental.

La **ciberdelincuencia**, el **secuestro de los datos**, (como la reciente campaña de WannaCry) el **ciberactivismo**[1], el **cibercrimen como servicio** o la **publicidad dañina** son otros de los aspectos analizados por el *Informe de Ciberamenazas y Tendencias. Edición 2017*[2] que, por noveno año consecutivo, elabora el CCN-CERT y cuyo resumen ejecutivo tienen ahora en sus manos. Un documento que se espera sirva para conocer algo más de las ciberamenazas existentes y, de este modo, afrontar de un modo más eficaz la difícil tarea de la ciberseguridad.

[1] Hacktivismo o ciberactivismo. Activismo digital antisocial. Sus practicantes persiguen el control de ordenadores o sitios web para promover su causa, defender su posicionamiento político, o interrumpir servicios, impidiendo o dificultando el uso legítimo de los mismos.
[2] El Informe completo (CCN-CERT IA-16/17 Ciberamenazas y Tendencias. Edición 2017) está disponible en el portal https://www.ccn-cert.cni.es

2 CIBERINCIDENTES
¿QUÉ ESTÁ PASANDO?

En los siguientes epígrafes se desarrollan los ciberincidentes más significativos de 2016, agrupados por las motivaciones de los agentes de la amenaza

CIBERESPIONAJE

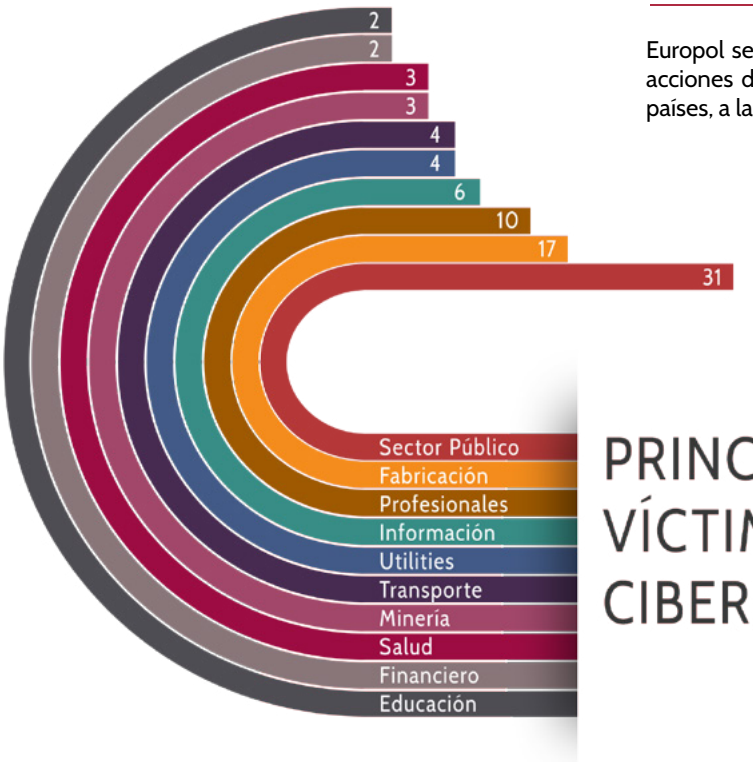
Para España, como para el resto de los países de nuestro entorno, el ciberespionaje sigue constituyendo la mayor amenaza para la seguridad nacional. Durante 2016, los servicios de inteligencia occidentales observaron un importante crecimiento del **ciberespionaje económico**, especialmente dirigido a las industrias de los sectores de **defensa**, **alta tecnología**, **industria química**, **energía y salud**, persiguiendo el acceso a desarrollos avanzados teniendo su origen en Estados y empresas.

De igual importancia es el **ciberespionaje político**, con origen en los Servicios de inteligencia que persigue información de naturaleza política, económica o estratégica, así como planes de desarrollo y posiciones nacionales en torno a debates o negociaciones abiertas.

En el siguiente gráfico se puede ver los sectores que, según la compañía Verizon, han sufrido un mayor número de ataques.

CIBERDELINCUENCIA

Europol señala que en 2016 se produjo un aumento sustancial de las acciones delictivas en el ciberespacio, llegando a superar, en algunos países, a la delincuencia tradicional.



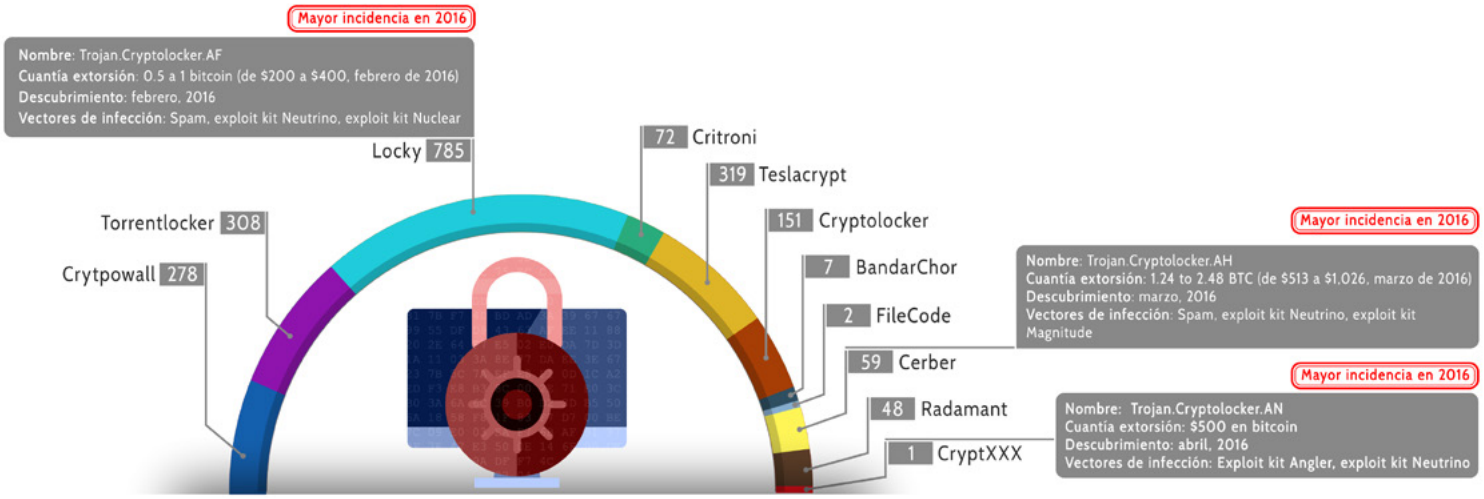
PRINCIPALES VÍCTIMAS DEL CIBERESPIONAJE

RANSOMWARE Y CRYPTOWARE

El **ransomware**[3] ha sido el vector de ataque **que más creció durante 2016**, con cerca de 150.000 casos por mes. Lo hizo de manera exponencial, en todo el mundo, sobre todo en los sectores de energía (persiguiendo la interrupción del suministro), gubernamental, sanitario y telecomunicaciones.

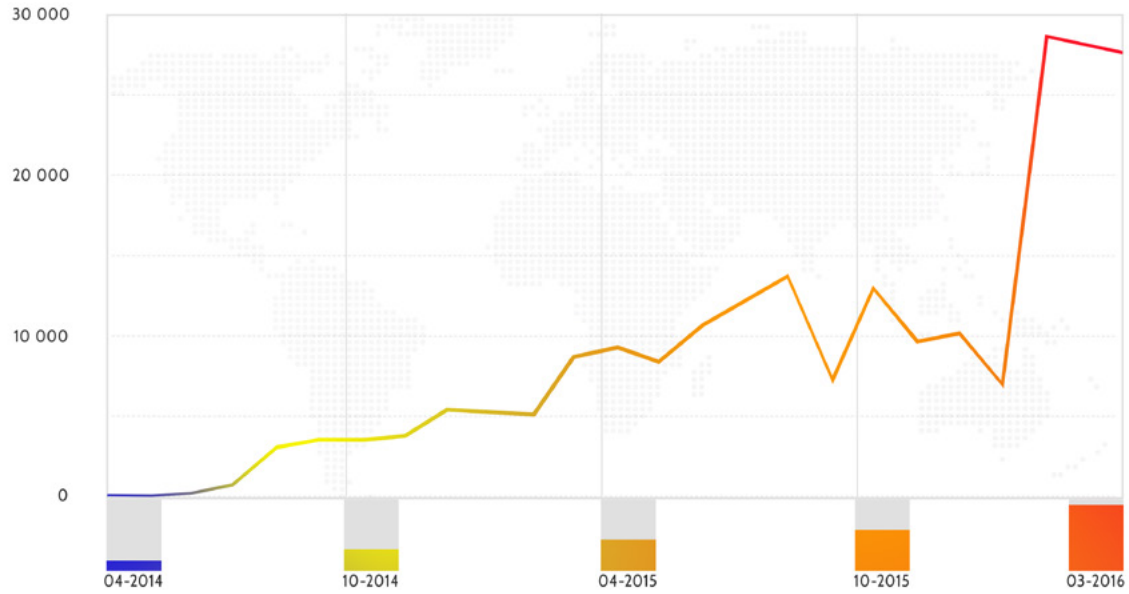
Los ataques **se están volviendo cada vez más dirigidos**, utilizando técnicas de **ingeniería social**, afectando a los sistemas de copia de seguridad, que hace imposible en muchos casos la recuperación de la información.

Sólo en España, y desde el CCN-CERT, se gestionaron en 2016 un total de 2.030 incidentes de distintos tipos de ransomware, un 375% más que en 2015



Nº DE INCIDENTES RANSOMWARE (CCN-CERT)

DISPOSITIVOS MÓVILES COMPROMETIDOS[4]



[3] 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.
[4] Fuente: Kaspersky Lb

CAMPAÑA WANNACRY

Mención especial requiere la campaña de **ransomware WannaCry**, detectada el 12 de mayo de este 2017 y que alcanzó en todo el mundo una repercusión mediática inusitada hasta el momento. Esta campaña utilizó el exploit[5] que aprovechaba la vulnerabilidad de Microsoft (MS17-010) y cuyo parche había sido publicado por la compañía el 14 de marzo.

En nuestro país, el CCN-CERT, que lanzó en 24 horas la primera vacuna frente a este código dañino (NoMoreCry Tool), detectó 239 direcciones IP que habían intentado contactar con uno de los dominios dañinos identificados.

Del mismo modo, y a pesar de las medidas de prevención y mitigación publicadas por el propio CERT Gubernamental Nacional el mismo día del ataque[6], cinco días después se tenía constancia de la existencia de 2.774 direcciones IP, con origen en España, vulnerables todavía al exploit utilizado.

WANNACRY

PUBLICIDAD DAÑINA

El año 2016 fue especialmente significativo en ciberincidentes provocados por la presencia de publicidad dañina en páginas web muy conocidas. En muchas ocasiones, la metodología seguida por los atacantes sugiere la presencia de ciberdelincuentes.

ATAQUES A LAS ENTIDADES FINANCIERAS

Se vienen produciendo menos ataques a usuarios finales, pero el ransomware y RAT *(Remote Access Tools)* dirigidos a las propias entidades[7] se han incrementado.

Además, siguen las campañas de phishing[8] para obtener credenciales, que luego son vendidas en la Internet profunda *(deep web)*, con una tasa de éxito elevada por la cuidada elaboración del correo de engaño.

[5] Programa que explota o aprovecha una vulnerabilidad de un sistema informático en beneficio propio. **Exploit día cero** Aprovechamiento de una vulnerabilidad inmediatamente después de haber sido descubierta. Se beneficia del lapso de tiempo requerido por los fabricantes para reparar las vulnerabilidades reportadas.
[6] https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
[7] Como se observó en el caso de Carnabak, donde las transacciones de la red internacional Swift fueron objeto de los ataques.
[8] Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.
[9] Fuente: TrendMicro.

SUSTRACCIÓN DE INFORMACIÓN

Muchos fueron los casos durante 2016 con propósitos económicos, obtención de credenciales o para desarrollar acciones de contraespionaje o chantaje[10]: **centros hospitalarios, formaciones políticas**[11] y gobiernos de países occidentales, **hostelería y comercio** o **intercambiadores de divisas virtuales**. Europol indica que hasta el 89% del robo de datos tiene un motivo financiero o de espionaje.

BRECHAS DE SEGURIDAD MÁS SIGNIFICATIVAS EN 2016[12]

Organización	Sector	País	Origen de brecha	Registros comprometidos	Datos comprometidos
Fling	Adultos		Personal externo	40 000 000	email, IP, datos
T Mobile	Telecomunicaciones		Personal interno	1 500 000	No divulgada
Kiddicare	Comercio		Personal externo	794 000	Nombre, email, teléfono
Nulled.io	Criminal		Desconocido	474 000	Credenciales, email, IP, mensajes
Kinoptic	Tecnología		Pérdida accidental	198 000	Credenciales, email, contraseñas hasheadas
Rosebutt Board	Adultos		Personal externo	107 000	Credenciales, IP, contraseñas hasheadas
Landesbank Berlin y otros	Financiero		Personal externo	85 000	Tarjetas de crédito
Swiss People's Party (SVP)	Gubernamental		Personal externo	50 000	Nombre, email
Islamic State	Militar		Personal interno	22 000	Nombre, dirección, teléfono, datos personales
Greenwich University	Educación		Personal externo	21 000	Nombre, email, datos personales, firma
Engitel	Tecnología		Ciberactivistas	20 000+	Credenciales, email
Faithless	Entretenimiento		Personal externo	18 000	email
National Childbirth Trust	Otros		Personal externo	15 000	email, credenciales
ShOping.su	Criminal		Personal externo	16 500	Credenciales, email y tarjetas
Liverpool University	Educación		Personal externo	6 500	Nombre, email

[10] Ataques a la U.S. Office Personnel Management (OPM), en junio de 2015, en el que fueron sustraídos datos de cuatro millones de empleados públicos o el robo de datos personales del website de citas Ashley Madison, en el que fueron sustraídos más de treinta millones de datos de personas.
[11] Tales como el Partido Demócrata norteamericano.
[12] Breach Level Index, Data Breach Statistics, (véase: http://www.breachlevelindex.com/#!breach-database)

USUARIOS PARTICULARES QUE HAN SUFRIDO ALGÚN CIBERINCIDENTE EN 2016[13]

Interrupción de sistemas

ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)

Durante 2016, muchas organizaciones de todo el mundo fueron víctimas de ataques de denegación de servicio (DoS), donde cada vez es más frecuente que escondan una extorsión: se insta a las víctimas a pagar un rescate a cambio de no iniciar un ataque de este tipo[14].

SABOTAJE DIGITAL

El mayor peligro es cuando el ataque está dirigido por un Estado[15], aunque hasta el momento los más numerosos han tenido su origen en antiguos empleados descontentos, con credenciales de acceso. Las acciones más comunes son el borrado de información y la destrucción/deterioro de soportes de almacenamiento.

DESFIGURACIONES

La desfiguración de páginas web sigue constituyendo una actividad habitual. Son acciones que, generalmente, encuentran su origen en motivos ideológicos o como medio para demostrar públicamente las capacidades de los atacantes.

INFRAESTRUCTURAS CRÍTICAS

Los ataques a los Sistemas de Control Industrial (SCI) se consideran una amenaza potencial por los procesos que gestionan. Los incidentes confirmados a estos sistemas todavía son escasos, pero se detectan muchas instalaciones con configuraciones inseguras o con conexiones a Internet sin la

Se detectan muchas instalaciones industriales con configuraciones inseguras o con conexiones a Internet sin la adecuada vigilancia

[13] Fuente: ONTSI: Estudio sobre la Ciberseguridad y confianza en los hogares españoles (Nov., 2016)
[14] Un ejemplo de organización para la extorsión en base a amenazas DDoS es el grupo llamado DD4BC *(DDoS for bitcoin)*.
[15] Como los ataques a compañías de electricidad de Ucrania, que ocasionaron que entre 700.000 y 1,4 millones de personas se quedaran sin energía eléctrica.

Costes de los ciberincidentes y su gestión

Los incidentes de seguridad tienen un coste global, derivado de varios costes parciales: económicos directos, de servicio, de imagen y reputación, por sanciones, etc. Sólo en los Estados Unidos y en 2015, el *Internet Crime Complaint Center* (IC3) del FBI, gestionó 288.012 denuncias individuales de ciberincidentes en Internet con unas pérdidas estimadas de 1.070 millones de dólares. La cifra de pérdidas en todo el mundo, se cifra en unos 400.000 millones de dólares[16].

Por lo que respecta al **ransomware**, el rescate promedio exigido por los atacantes aumentó en 2016, elevándose a 679 dólares, frente a los 294 dólares de 2015. En 2016, también se registró un nuevo récord con la familia **Cryptolocker**, al solicitar un rescate de 13 bitcoin[17] por ordenador infectado (unos 5.083 dólares)[18].

[16] Fuente: Khoo Boon Hui (Ex presidente de INTERPOL). "Los cibercriminales se lucran en Internet". Fundación Innovación Bankinter – Fundación Future Trends Forum.
[17] Moneda digital o criptomoneda, con un valor aproximado a los 39 dólares por unidad.
[18] Fuente: Symantec: Special Report: Ransomware and Businesses, 2016.

AGENTES DE LA AMENAZA

	ORIGEN	MOTIVACIÓN
1	ESTADOS	Mejorar su posición geopolítica o estratégica
2	ORGANIZACIONES CRIMINALES	Beneficio económico (directo e indirecto)
3	ORGANIZACIONES PRIVADAS	Ciberespionaje: obtención de información de valor.
4	CIBERTERRORISTAS	Alterar el normal desenvolvimiento social, atemorizar a la población o influir en las decisiones políticas.
5	CIBERYIHADISTAS	Propaganda, reclutamiento
6	CIBERACTIVISMO	Ideología
7	CIBERVÁNDALOS Y SCRIPT KIDDIES[19]	Evidenciar vulnerabilidades, piratería, diversión, retos.
8	ACTORES INTERNOS	Venganza, beneficio económico, motivos ideológicos.
9	CIBERINVESTIGADORES	Evidenciar debilidades, autoafirmación.

NIVEL DE PELIGROSIDAD

[19] Son 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

VÍCTIMAS


SECTOR PÚBLICO
ORGANIZACIONES PRIVADAS
CIUDADANOS
Ciberespionaje político
Capacidades ofensivas
Ciberespionaje económico
Capacidades ofensivas
Ciberespionaje
Robo y publicación o venta de información
Manipulación de la información
Interrupción de sistemas
Toma de control de sistemas
Robo y publicación o venta de información
Manipulación de la información
Interrupción de sistemas
Toma de control de sistemas
Robo y publicación o venta de información
Manipulación de la información
Interrupción de sistemas
Toma de control de sistemas
Ciberespionaje industrial o económico
Abuso o reventa de información corporativa
Interrupción / toma de control de sistemas
Interrupción / toma de control de sistemas
Propaganda / Reclutamiento
Propaganda / Reclutamiento
Propaganda / Reclutamiento
Robo y publicación de información
Desfiguraciones
Interrupción de sistemas
Toma de control de sistemas
Robo y publicación de información
Desfiguraciones
Interrupción de sistemas
Toma de control de sistemas
Robo de información
Interrupción de sistemas
Robo de información
Interrupción de sistemas
Robo de información
Robo y publicación o venta de información
Interrupción de sistemas
Robo y publicación o venta de información
Interrupción de sistemas
Publicación de información
Publicación de información
Existen claros desarrollos relacionados con la amenaza.
Las medidas desplegadas tienen un efecto limitado en la amenaza.
El número de incidentes derivados de la amenaza ha sido significativo.
Se han observado nuevas tendencias o fenómenos asociados con la amenaza.
Existe un conjunto de medidas limitadas para eliminar la amenaza
El número de incidentes derivados de la amenaza no ha sido especialmente significativo
No han aparecido nuevas amenazas.
Existen suficientes medidas para eliminar la amenaza
No han existido incidentes apreciables derivados de la amenaza.

3 AGENTES DE LA AMENAZA ¿QUIÉN NOS ATACA?

LOS ESTADOS

La mayor amenaza para la ciberseguridad nacional lo constituyen las acciones dirigidas por los Estados, muy especialmente aquellas que tienen su origen en los Servicios de Inteligencia. Son una alternativa real al espionaje tradicional debido a su bajo coste, a la dificultad de probar su autoría y al importante volumen de información que puede obtenerse por esta vía.

Las motivaciones de los Estados serían:

- Obtener información de la víctima sobre seguridad y defensa nacional, propiedad intelectual e inteligencia sobre las capacidades militares (explotándolas posteriormente, después de conocer sus vulnerabilidades).
- Impedir el uso de los canales de comunicación del adversario en el ciberespacio.
- Realizar actividades subversivas en situaciones de crisis o conflicto, o realizar acciones de influencia.

España ha recibido ataques especialmente dirigidos a las industrias de Defensa, compañías tecnológicas y entidades representativas del sector público.

Por otro lado, los Estados siguen invirtiendo en el desarrollo de capacidades **ciberofensivas**, realizadas generalmente a través de los Servicios de Inteligencia y unidades específicas de ciberdefensa de las Fuerzas Armadas.

Durante 2016 se consolidó el concepto de guerra híbrida[20], una de las amenazas emergentes más relevantes. Grupos como APT28, asociado con la agencia de inteligencia militar rusa (GRU), realizaron diversas acciones comprendidas en este concepto.

Los últimos años han evidenciado que las amenazas a los sistemas de información, siguen creciendo, y lo hacen en tipología, volumen, sofisticación y peligrosidad

ORGANIZACIONES CRIMINALES

Buscan la obtención de un beneficio económico directo (sustracción de credenciales) o indirecto (a través de extorsiones), tanto a organizaciones como a individuos. En este último caso, el **ransomware** y las amenazas relacionadas con ataques **DoS**[21], fueron los métodos más utilizados.

Su nivel de conocimientos es muy variado, y abarca todo el espectro desde los especialistas (con alto nivel de profesionalidad y de innovación) hasta grupos de bajo nivel. Así, la utilización del cibercrimen como un servicio ***(Cybercrime-as-a-service)*** sigue incrementándose, utilizando la Internet profunda (deep web) para el intercambio de herramientas y la planificación de ataques.

Se observan servicios como: venta de código dañino listo para su uso (incluido ransomware), información robada de tarjetas de crédito, correos electrónicos y redes sociales, herramientas para el desarrollo de ataques de denegación de servicio o herramientas de acceso remoto (RAT) diseñadas para la comisión de acciones delictivas.

El uso de técnicas para conseguir el **anonimato** (intermediarios o proxies, redes privadas virtuales y TOR[22]) en conjunción con el empleo de **bitcoins** dificultan extraordinariamente las labores de investigación.

Se ha observado un importante crecimiento en la cooperación, incluso con presencia física, entre distintos grupos de ciberdelincuentes[23].

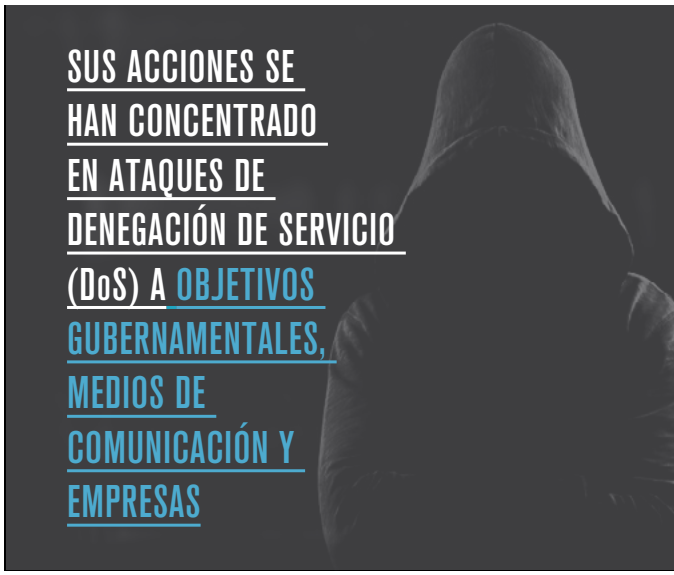
[20] Operación dirigida por un Estado que utiliza tácticas abiertas y encubiertas con el objetivo de desestabilizar otros Estados y polarizar a la población civil. Incluye una gran variedad de herramientas como diplomacia y acciones de inteligencia tradicional, actos subversivos y de sabotaje, influencia política y económica, instrumentalización del crimen organizado, operaciones psicológicas y propaganda.
[21] Los atacantes más conocidos han sido DD4BC y Armada Collective.
[22] 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 a los problemas de privacidad de Internet. 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.
[23] Campaña de código dañino Dyre, en la que se pusieron de acuerdo varios grupos de cibercriminales en un edificio de oficinas en Rusia. http://tweakers.net/nieuws/108009/verspreiding-financiele-dyre-malware-gestopt-door-russische-autoriteiten.html

ciberactivismo[24]

Estos grupos justifican sus acciones con motivos ideológicos y su propósito es visibilizar o reivindicar una causa. Está considerado como una forma de activismo insurgente.

Sus acciones se han concentrado en ataques de denegación de servicio (DoS) a objetivos gubernamentales, medios de comunicación y organizaciones privadas y en desvelar determinados comportamientos o datos personales de instituciones gubernamentales. Sus capacidades son muy variadas, llegando a alcanzar un alto grado de sofisticación.

En España, continúa sin traducirse en un colectivo estable desde 2012, cuando la policía desarticuló la infraestructura de **Anonymous** (#OpSpain). El ecosistema ciberactivista está caracterizado por una baja densidad de identidades de propaganda sin apenas capacidades operativas, con la excepción de "**La 9ª Compañía de Anonymous**", que ha comprometido sitios web de ayuntamientos, medios de comunicación, empresas y cámaras de comercio.



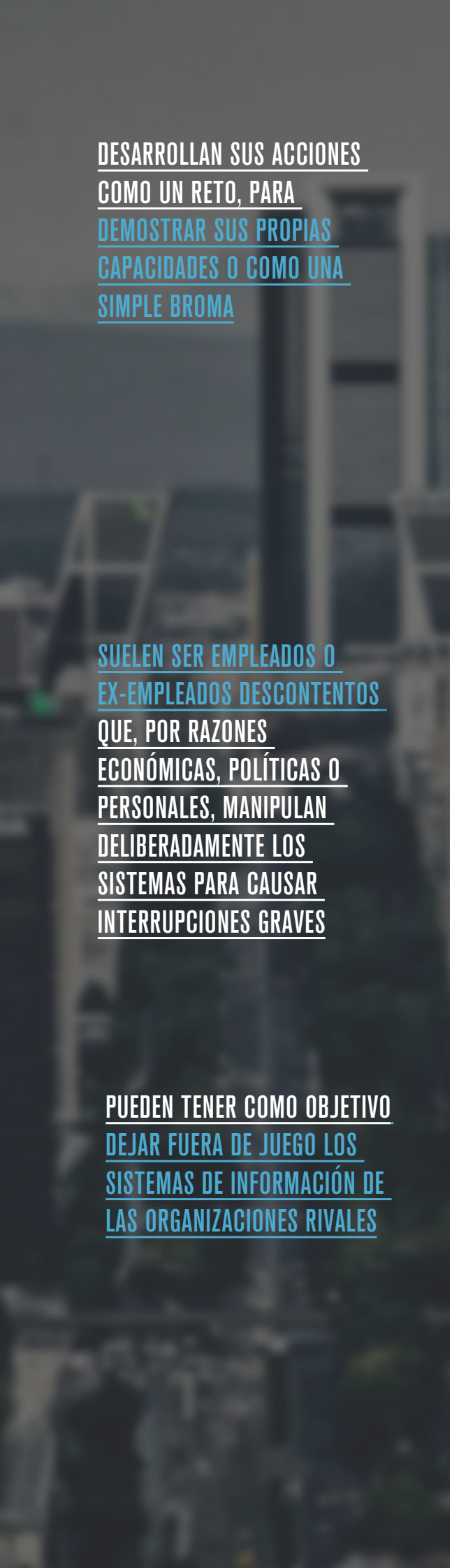
ciberterrorismo

El terrorismo yihadista también emplea la dimensión del ciberespacio para tareas que no implican la comisión directa de un atentado, sino labores de adoctrinamiento, reclutamiento y logística.

El **uso de Internet** representa una operativa de uso intensivo por grupos yihadistas, principalmente por el **Daesh**[25], pero también por **Al Qaeda**, **Boko Haram** o **Al Shabaab** hasta tal punto que grupos de nueva creación, como el aparecido en 2016 en Egipto, **Harakat Sawa'd Misr**, ya nacen con su propio sitio web [https://hasam.org]. No obstante, no se han apreciado acciones terroristas en el ciberespacio, pero sí actividad de grupos u organizaciones terroristas en él.

La mayor parte de los denominados grupos Ciberyihadistas[26] que, además de provocar desfiguraciones de páginas web[27], pequeños ataques DDoS o contra cuentas de redes sociales, se ha concentrado en ocultar la información intercambiada a través de canales de comunicación cifrados.

[24] Existe un anexo del Informe general centrado en el Hacktivismo y Ciberyihadismo CCN-CERT IA-04/17 Hacktivismo y Ciberyihadismo 2016
[25] Al-Dawla al –islamiya fil Iraq wa al Sham (o ISIS en inglés).Estado Islámico de Iraq y el "sham" que comprende Iraq, Siria y parte de El Líbano.
[26] Los actores potenciales más significativos del ciberyihadismo son: Al Qaeda, Al Shabaab, Boko Haram e ISIS (o Daesh). Ver: "The Anatomy of Cyber-Jihad". J. Scott y D. Spaniel (2016).
[27] Como las que pudieron observarse tras los atentados de París.



DESARROLLAN SUS ACCIONES COMO UN RETO, PARA DEMOSTRAR SUS PROPIAS CAPACIDADES O COMO UNA SIMPLE BROMA

SUELEN SER EMPLEADOS O EX-EMPLEADOS DESCONTENTOS QUE, POR RAZONES ECONÓMICAS, POLÍTICAS O PERSONALES, MANIPULAN DELIBERADAMENTE LOS SISTEMAS PARA CAUSAR INTERRUPCIONES GRAVES

PUEDEN TENER COMO OBJETIVO DEJAR FUERA DE JUEGO LOS SISTEMAS DE INFORMACIÓN DE LAS ORGANIZACIONES RIVALES

CIBERVÁNDALOS Y SCRIPT KIDDIES

Durante 2016 se observó un importante crecimiento de las acciones de estos agentes, motivadas por el incremento de herramientas para la perpetración de ataques. Estos actores desarrollan sus acciones como un reto, para demostrar sus propias capacidades o como una simple broma.

Se han utilizado los llamados **Booter-Services**[28] (**DDoS-As-A-Service**) como mecanismos para la perpetración de ataques DDoS.

Como ejemplo: el grupo denominado "Crackas with attitude", que actuó contra directivos de ciertas unidades de inteligencia norteamericanas.

ACTORES INTERNOS Y CIBERINVESTIGADORES

Suelen ser empleados o ex-empleados descontentos que, por razones económicas, políticas o personales, manipulan deliberadamente los sistemas para causar interrupciones graves, dañar los sistemas de almacenamiento o apoderarse de información sensible.

Los ciberinvestigadores al perseguir el descubrimiento de vulnerabilidades y no respetar la difusión responsable mostrando públicamente un inadecuado nivel de seguridad hacen que, en muchas ocasiones, los sistemas descritos sean temporalmente vulnerables.

ORGANIZACIONES PRIVADAS

En ocasiones pueden tener como objetivo dejar fuera de juego los sistemas de información de los rivales, aunque lo más habitual es que tales ataques persigan obtener información de la competencia para usarla en su propio beneficio, incluso, para venderla a terceras partes. Esto es lo que suele denominarse ciberespionaje industrial[29].

[28] Es un servicio ofrecido por ciberdelincuentes que ejecutan ataques de denegación de servicio distribuido (DDoS) contra objetivos solicitados por sus clientes que pagan una cantidad económica por el encargo.
[29] En Estados Unidos se produjo un ataque de los empleados de una empresa proveedora de productos textiles a otra empresa de la competencia (véase: https://www.security.nl/posting/453200/IT-directeur+Amerikaans+bedrijf+hackte+server+concurrent

4 VULNERABILIDADES

¿POR QUÉ ME ATACAN?

SOFTWARE

La industria del software se parece cada vez más a una cadena de montaje en la que el producto obtenido es el resultado de reutilizar componentes ya existentes. Si alguno de los componentes presenta una vulnerabilidad, el resultado final será asimismo vulnerable[30].

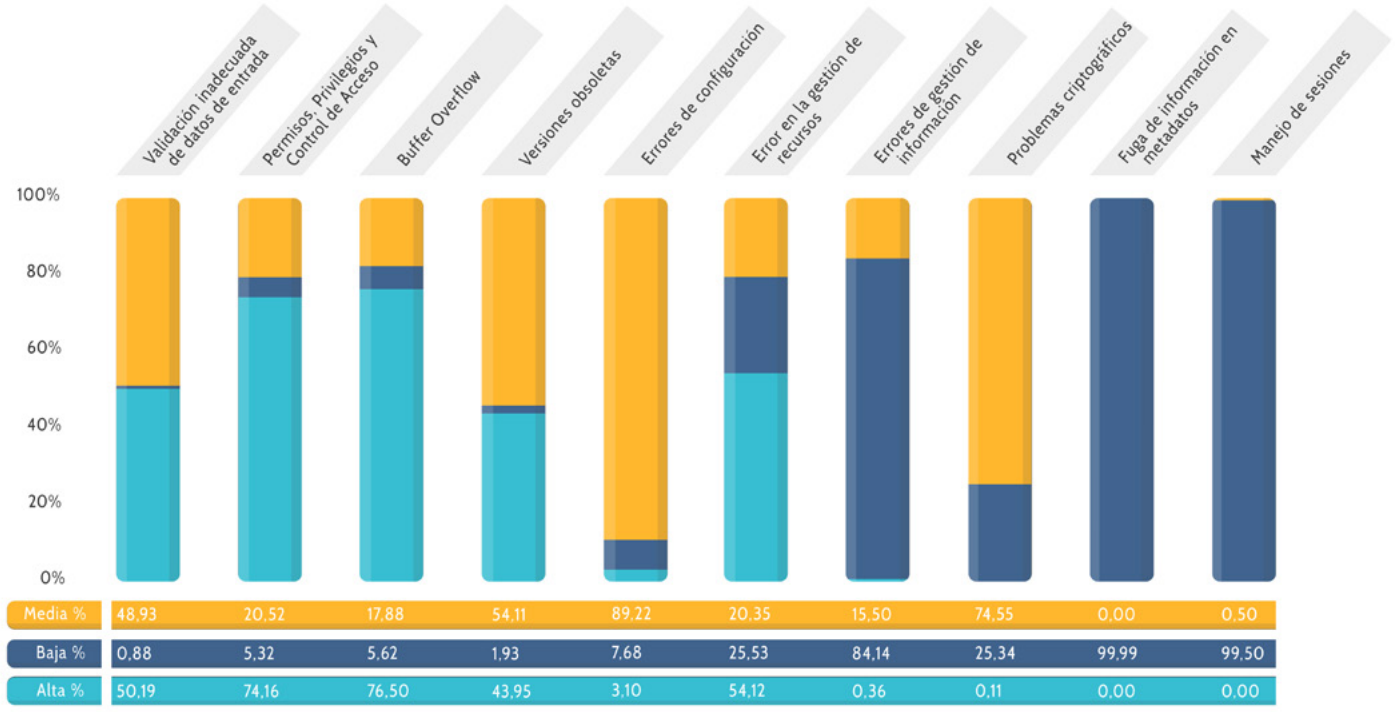
El número de vulnerabilidades sigue en permanente crecimiento

Otros aspectos a tener en cuenta:

- La enseñanza reglada de programación todavía presta poca atención a la ciberseguridad. Prima la funcionalidad de un software y su velocidad de cómputo frente a un comportamiento seguro.
- La inseguridad del software se vuelve especialmente delicada en los **Sistemas de Control Industrial** que operan durante mucho tiempo sin recibir las actualizaciones necesarias.
- Muchas brechas de seguridad son debidas a vulnerabilidades que llevaban tiempo siendo conocidas, pero las organizaciones responsables no las actualizan permitiendo la aparición de herramientas (exploit) que las aprovechan (el caso de WannaCry es prueba palpable de ello).
- Todavía en muchas organizaciones la única medida de seguridad es el software antivirus, muchas veces desactualizado.
- La exhibición pública de determinadas vulnerabilidades pone en grave riesgo a los sistemas afectados y, en ocasiones, una exagerada publicidad hace pasar desapercibidas otras más críticas.

[30] La compañía de Taiwán D-Link, filtró de manera accidental una de sus claves de firma de software, lo que provocó que ciertos atacantes utilizarán firmas legítimas de D-Link para desplegar código dañino (http://www.theregister.co.uk/2015/09/18/d_link_code_signing_key_leak/).

SEVERIDAD DE LAS VULNERABILIDADES (SEGÚN CRITERIO CVSS[31])



	Validación inadecuada de datos de entrada	Permisos, Privilegios y Control de Acceso	Buffer Overflow	Versiones obsoletas	Errores de configuración	Error en la gestión de recursos	Errores de gestión de información	Problemas criptográficos	Fuga de información en metadatos	Manejo de sesiones
Media %	48,93	20,52	17,88	54,11	89,22	20,35	15,50	74,55	0,00	0,50
Baja %	0,88	5,32	5,62	1,93	7,68	25,53	84,14	25,34	99,99	99,50
Alta %	50,19	74,16	76,50	43,95	3,10	54,12	0,36	0,11	0,00	0,00

EN EL PORTAL DEL CCN-CERT[32], EN 2016, SE PUBLICARON UN TOTAL DE 3.773 VULNERABILIDADES DECLARADAS POR LOS SIGUIENTES FABRICANTES:

Fabricante	1er semestre	2do semestre	Total 2016
Adobe	29	10	39
Apple	21	17	38
Cisco	259	82	341
Debian	365	269	634
IBM	1.203	330	1.533
Microsoft	145	125	270
Oracle	5	2	7
Red Hat	229	206	435
Symantec	204	272	476
Total:	2.460	1,313	3,773

[31] *Common Vulnerability Scoring Systems*. Sistema de valoración para estimar el impacto derivado de vulnerabilidades identificadas en sistemas de información.
[32] https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades.html

USUARIO

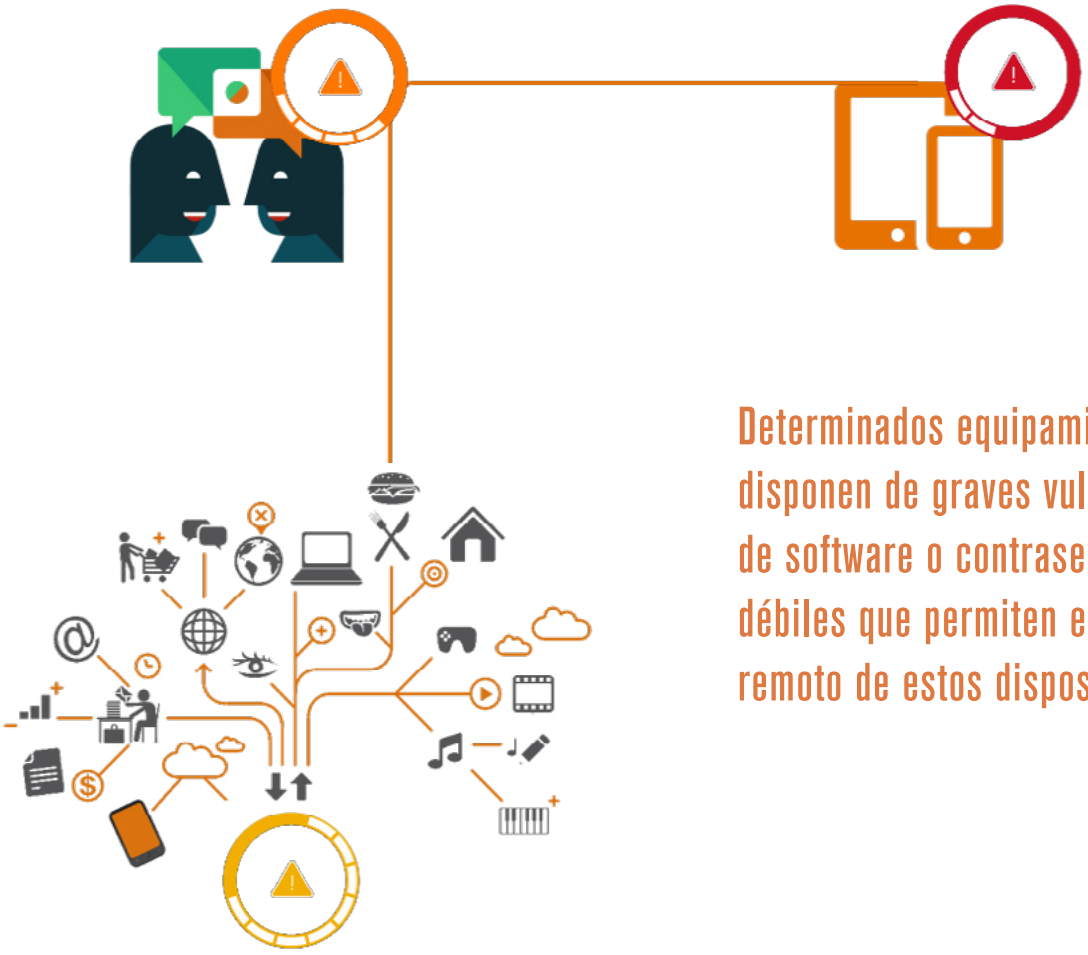
Con respecto a los usuarios, conviene recabar la atención en tres puntos: dispositivos móviles, ingeniería social e Internet de las Cosas.

Los **dispositivos móviles**, su ritmo de comercialización y vida útil (dos años es lo habitual), hace que muchos fabricantes dejan de publicar actualizaciones de seguridad para los productos más antiguos, lo que los convierte en víctimas para los ciberataques.

La **ingeniería social**, donde los atacantes continúan redoblando sus esfuerzos para engañar a sus víctimas. Muchos usuarios han caído en la trampa del correo electrónico dirigido (spear phishing) o, incluso, de llamadas telefónicas (cuyo incremento en 2016 ha sido espectacular). Cuando la ingeniería social se dirige específicamente a sectores individualizados el porcentaje de éxito crece exponencialmente.

El **Internet de las cosas (IoT)**, donde muchos fabricantes no parecen ser conscientes de los riesgos que supone su conexión a Internet y no implementan protocolos de comunicaciones seguros, incluso determinados equipamientos disponen de graves vulnerabilidades de software o contraseñas de acceso débiles que permiten el control remoto de estos dispositivos.

Cuando la ingeniería social se dirige específicamente a sectores individualizados el porcentaje de éxito crece exponencialmente



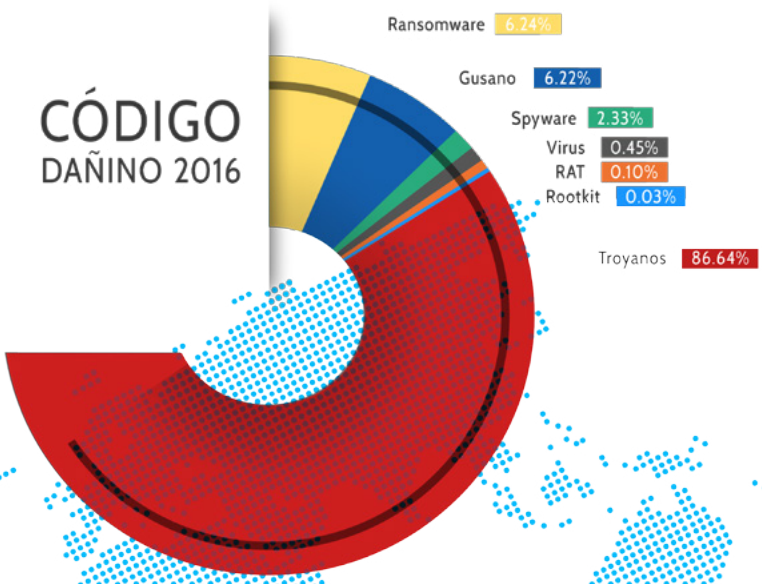
Determinados equipamientos disponen de graves vulnerabilidades de software o contraseñas de acceso débiles que permiten el control remoto de estos dispositivos

5 MÉTODOS DE ATAQUE

¿CÓMO ME ATACAN?

CÓDIGO DAÑINO

De su importancia y presencia en buena parte de los ciberincidentes, queda constancia en las cifras del CCN-CERT. Así, en 2016, de los 20.940 ciberincidentes gestionados en el sector público y en empresas de interés estratégico, el 53,6% (11.237) correspondían con la tipología de código dañino (y entre ellos el troyano[33]).



[33] 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)

En general, hay tres vías principales para la instalación de código dañino: correo electrónico con archivos adjuntos, sitios web que descargan este tipo de software o un híbrido de ambos (correos electrónicos con enlaces a páginas dañinas).

Tipología más usada:

- **Ransomware**: han empezado a afectar al sistema operativo de Apple (mac OS) y a otros servidores, como el código KeRanger, con lo que, además de obtener un rescate, los atacantes se han introducido en las redes de sus víctimas y han amenazado con divulgar sus datos personales.
- **Infección de páginas web de confianza para los usuarios**, como las tiendas oficiales de aplicaciones para dispositivos móviles o la infección de entornos de desarrollo, tanto de los propios fabricantes de software, como en los revendedores.
- Los **dispositivos móviles** continúan siendo un objetivo cada vez más utilizado por los atacantes. Aunque Android sigue constituyendo el objetivo principal, los ataques dirigidos a iOS siguen en aumento.

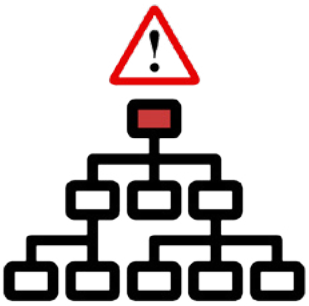
Herramientas de los ataques (exploit-kits)

La **comercialización de herramientas automáticas de ataque (exploits-kits)** sigue siendo una de las amenazas más significativas[34], afectando en la actualidad a ordenadores convencionales, teléfonos móviles y dispositivos de comunicaciones (routers[35]). No obstante, el 86% de los exploits contenidos en exploits-kits aprovechan vulnerabilidades del reproductor multimedia Flash Player.

Por otro lado, las **herramientas de acceso remoto** (RAT), sobre diferentes sistemas operativos, continúan constituyendo un procedimiento eficaz para atacar. El bajo coste de su adquisición (alrededor de cinco dólares en foros clandestinos), impulsa su utilización que incluso incluye soporte técnico.

[34] Ejemplos de ello han sido los exploits-kits Angler y Black Energy (al que se asoció la interrupción del suministro en las centrales eléctricas de Ucrania).
[35] Enrutador.

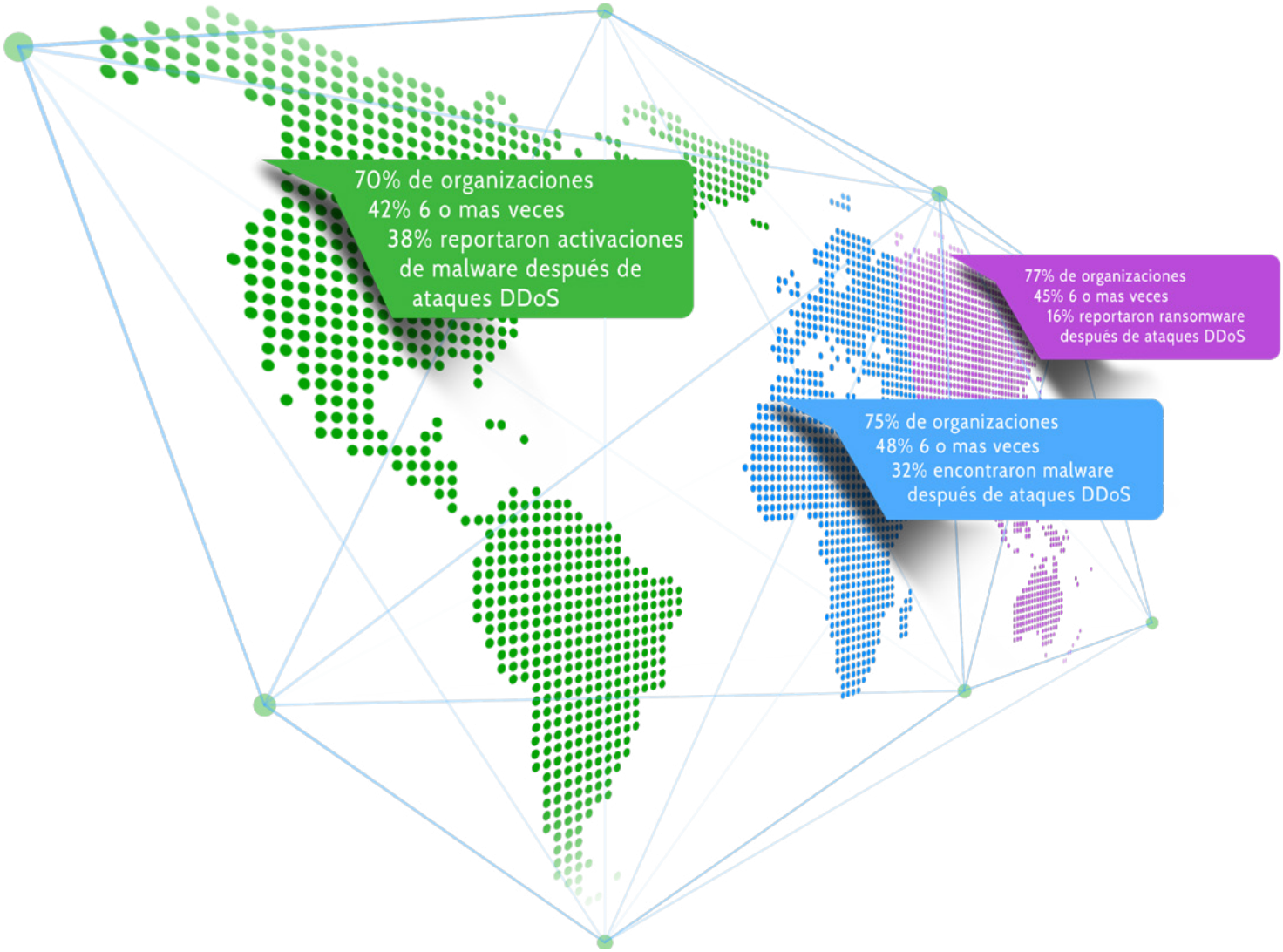
Ataques de denegación de servicio (DoS) y aplicaciones web



Los ataques de denegación de servicio registrados solo en el segundo trimestre de 2016, se incrementaron en un 129% respecto de los registrados en el mismo trimestre de 2015[36].

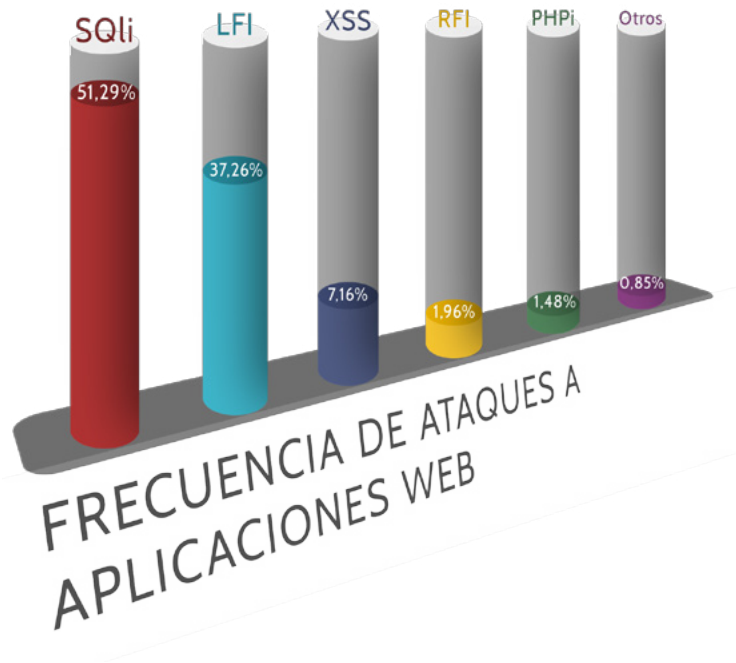
Según una encuesta realizada por la empresa Neustar, el 73 % de todas las organizaciones participantes sufrió un ataque DoS, el 49 % perdió, al menos, 100.000 dólares por hora durante los períodos punta y el 53 % tuvo un robo de datos como resultado de un ataque DoS.

INCIDENCIA DE ATAQUES DOS POR CONTINENTE



[36] Fuente: Akamai's State of the Internet / Security. Q2-Q4 2016 Security Report.

Durante 2016 continuaron buscando nuevas formas de expansión, abusando de las facilidades de aplicaciones y servicios legítimos como: NetBIOS, RPC, Sentinel, RPC Portmapper, DNSSEC, TFTP o Bittorrent. Además, ciertos tipos de dispositivos conectados a Internet, tales como la electrónica de red (routers, switches....), cámaras digitales con protocolo Internet (IP), discos duros de red e, incluso, impresoras de red, también se han usado para desarrollar ataques DoS.



Por lo que se refiere a **ataques a Aplicaciones Web**, los vectores de agresión más significativos fueron **inyección SQL**[37] y **Local File inclusión**[38], frente al resto. Entre ambos se acercan al 90% de la totalidad de los ataques.

Los vectores de agresión más significativos de ataques a aplicaciones web, fueron inyección SQL y Local File inclusión, frente al resto. Entre ambos se acercan al 90% de la totalidad de los ataques

[37] Structured Query Language; en español lenguaje de consulta estructurada: es un lenguaje de gestión de bases de datos relacionales.
[38] Inclusión de ficheros locales, es decir, ficheros que se encuentran en el mismo servidor de la web con este tipo de fallo, a diferencia de Remote File Inclusion que incluye ficheros alojados en otros servidores.

RESULTA PREVISIBLE EL AUMENTO DEL VOLUMEN DE CÓDIGO DAÑINO AVANZADO Y LOS CASOS DE ROBO DE DATOS USANDO SSL/TLS

OCULTACIÓN DEL ATACANTE Y ABUSO DE SERVICIOS

El interés del atacante es ocultar su identidad, eliminando las evidencias que hubiese podido dejar en los sistemas infectados utilizando, por ejemplo, los denominados **USBthief**, en los que el código dañino que contienen sólo puede ejecutarse desde la memoria USB original, sin dejar ninguna evidencia en el sistema comprometido.

También se han confirmado ataques a servicios muy populares, tales como Dropbox, Pinterest y Google Docs, aprovechando que el tráfico suele estar cifrado por defecto[39]. Los atacantes también se aprovecharon de las autoridades de certificación legítimas para obtener certificados digitales con los que aparentar una imagen de legalidad, así como de comunicaciones vía satélite para enmascarar la localización de los servidores de mando y control del ataque (C&C)[40].

Resulta previsible asimismo el aumento del volumen de código dañino avanzado y los casos de robo de datos usando SSL/TLS[41]. Todo ello significa que la gestión del tráfico cifrado está llamada a jugar un papel cada vez más importante en la protección de las infraestructuras.

PUBLICIDAD DAÑINA

La publicidad que se utiliza para infectar los ordenadores de la víctima continúa siendo muy utilizada. El denominado "adware"[42] ha seguido incrementándose y ha ido evolucionando hasta el **Malvertising-as-a-service (MaaS)**[43].

Si determinadas páginas web reciben diariamente cientos de miles de visitas, vemos que nos encontramos ante una amenaza de la mayor magnitud que permite, incluso, dirigir las infecciones hacía un sector concreto o que se encuentre específicamente interesado en un determinado tipo de producto.

Pese a todo, la protección contra la publicidad dañina no es fácil. El modelo de negocio sustentado en la publicidad web impediría, en muchos casos, el uso de sistemas de bloqueo de anuncios (ad-blockers).

[39] Por ejemplo, Hamertoss, la puerta trasera del grupo denominado APT29, usó Twitter para comunicarse con sus sistemas C&C.
[40] Command and control.
[41] Secure Sockets Layer. Protocolo de cifra que permite el intercambio seguro de información entre dos extremos, predecesor de TLS (Transport Layer Security).
[42] Software publicitario. Aplicaciones que durante su funcionamiento despliegan publicidad en ventanas emergentes o barras de herramientas a cambio de la gratuidad en su utilización. La publicidad normalmente permite visitar la página web del anunciante, por lo que requiere conexión a Internet para funcionar. Se diferencian de los programas gratuitos (freeware) en que incorporan publicidad. La mayoría de los programas publicitarios son confiables, pero en ocasiones algunos de ellos son utilizados con fines poco éticos llegando a comportarse como auténticos programas espías para controlar movimientos de los usuarios.
[43] Código dañino insertado en publicidad como servicio.

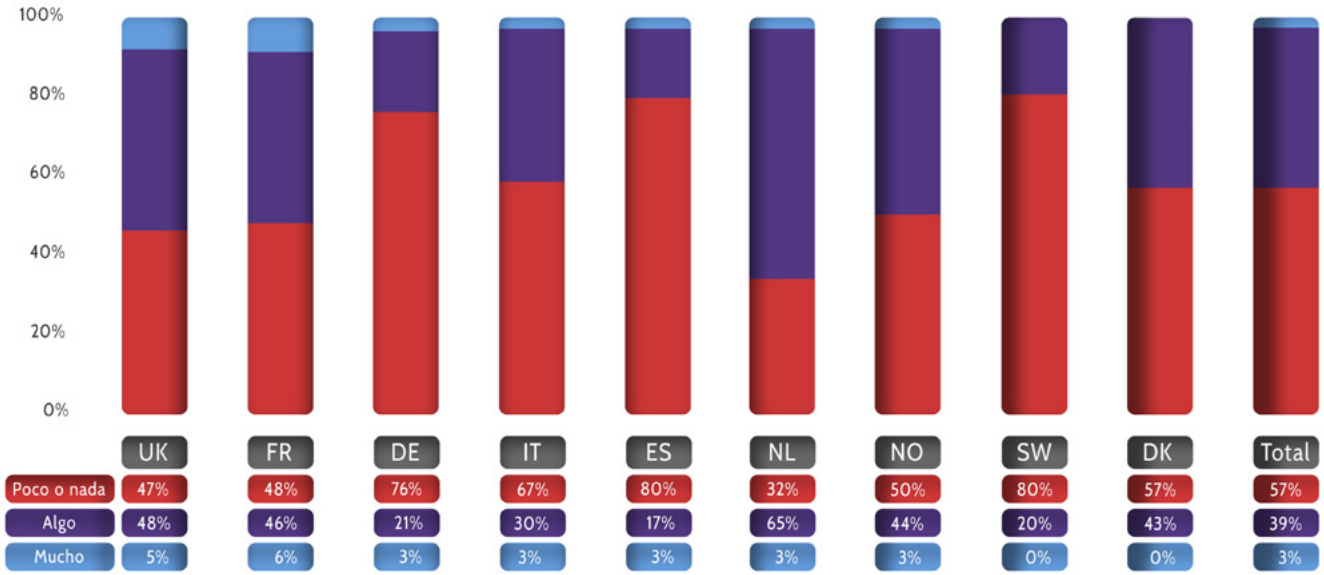
6 MEDIDAS

¿QUÉ HACER PARA PROTEGERME?

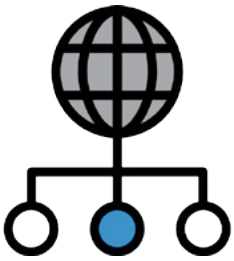
Factor humano

La concienciación en materia de ciberseguridad sigue siendo una asignatura pendiente en muchos países. La figura siguiente (encuesta de Lloyd's), muestra el grado de concienciación de los empresarios de ciertos países europeos sobre tales extremos.

GRADO DE CONCIENCIACIÓN EN LAS EMPRESAS



	UK	FR	DE	IT	ES	NL	NO	SW	DK	Total
Poco o nada	47%	48%	76%	67%	80%	32%	50%	80%	57%	57%
Algo	48%	46%	21%	30%	17%	65%	44%	20%	43%	39%
Mucho	5%	6%	3%	3%	3%	3%	3%	0%	0%	3%



La sensibilización, por sí sola, no es suficiente. Según un informe de Verizon, los usuarios abren el 30% de los correos electrónicos sospechosos (phishing) y hacen clic en el 12 % de los ficheros adjuntos.

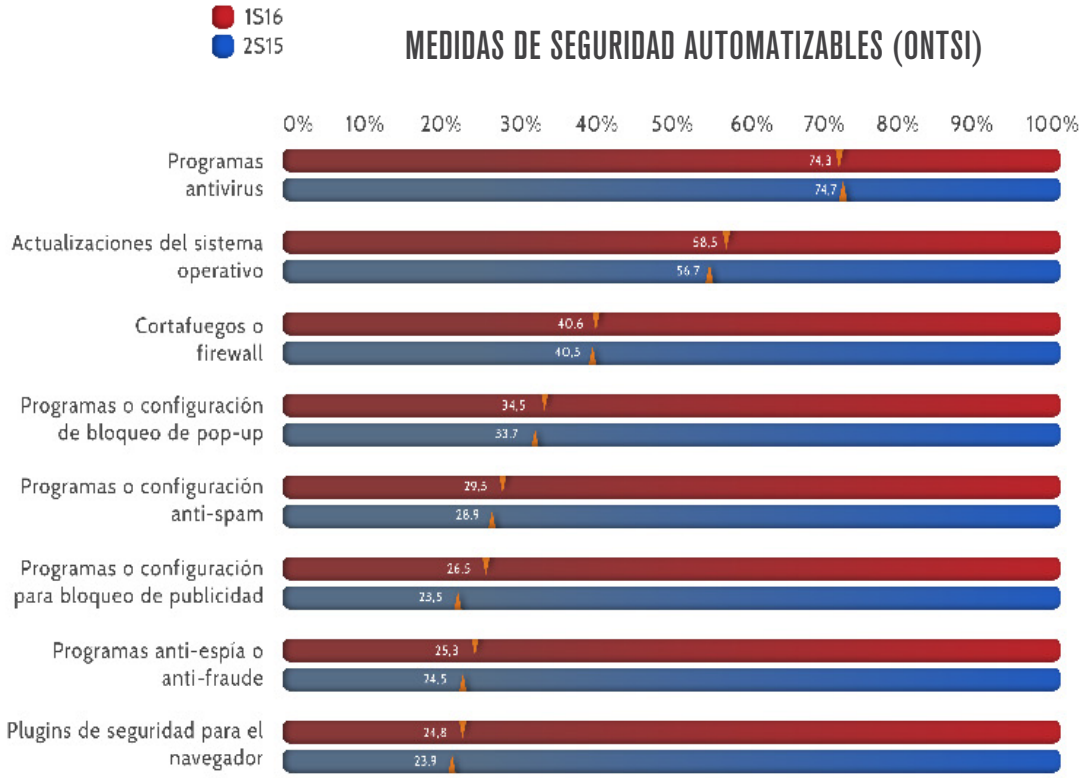
Además, la actual escasez de profesionales en materia de ciberseguridad es un problema. Por ello las organizaciones deben hacer un esfuerzo adicional de formar al personal contratado. Existe una ausencia significativa de personal con perfil de monitorización de sistemas, investigación de incidentes, análisis forense o implementación de configuraciones de seguridad.

Factor tecnológico

Pese a que el usuario constituye en muchas ocasiones el eslabón más débil de la cadena en un ciberataque, la tecnología sigue siendo indispensable para garantizar la seguridad.

Uno de los elementos más delicados lo constituyen las **versiones sin soporte** del software o la ausencia de un consenso respecto a qué configuraciones de seguridad serían las más idóneas para prevenir ataques.

La **utilización de estándares, como el Esquema Nacional de Seguridad (ENS)**[44], puede ayudar de manera significativa a identificar tales medidas. Es más que recomendable el empleo de las configuraciones propuestas en las diferentes series de guías de seguridad del Centro Criptológico Nacional (CCN-STIC).



Conviene reseñar, en este sentido, que el Centro Criptológico Nacional tiene entre sus funciones la protección y fomento de tecnología segura. Coordina la promoción, desarrollo, obtención, adquisición y puesta en explotación y uso de tecnologías de seguridad; además de valorar y certificar productos de cifra y acreditar sistemas para manejar información de forma segura; constituyendo el **Organismo de Certificación**[45] del Esquema Nacional de Evaluación y Certificación de la Seguridad, de aplicación a productos y sistemas en su ámbito.

De hecho, está prevista la publicación de un **Catálogo de Productos recomendados**, en el que se ofrecerá un listado de productos de seguridad de las TIC supervisado por el CCN que proporcionará un nivel mínimo de confianza al usuario final y a la organización que los emplee.

[44] El ENS desarrollado por el RD 3/2010, de 8 de enero, es de aplicación al sector público español (Ley 40/2015, de 1 de octubre).
[45] Desde donde se aplica el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por Orden PRE/2740/2007, de 19 de septiembre.

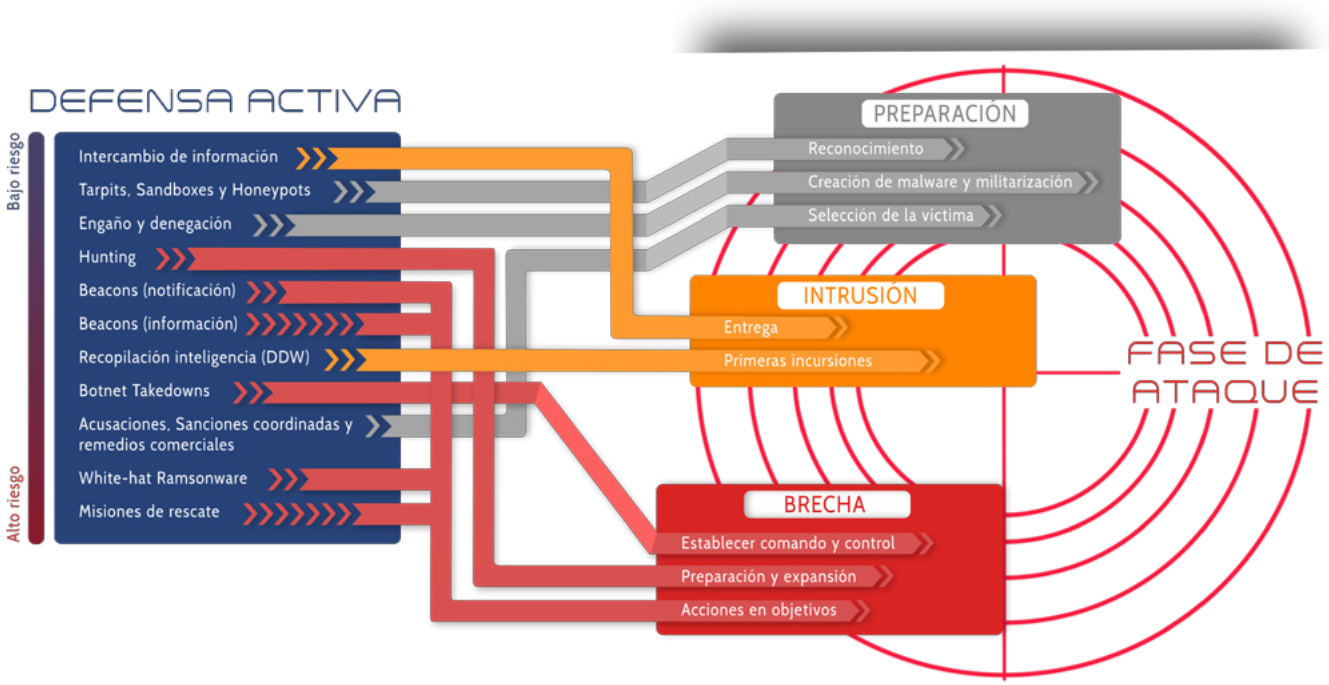
Factor económico y metodológico

Cada día se plantean nuevos peligros en el ciberespacio que difícilmente se pueden cuantificar. En este contexto las **pólizas de ciberriesgos** se erigen como defensa de primer orden que, junto con la concienciación de los trabajadores y el incremento de la ciberseguridad corporativa, tendrán beneficiosos efectos sobre los mercados nacionales e internacionales.

Finalmente, 2016 colocó en el panorama mundial la llamada **Defensa Activa**. Estas actividades pueden cruzar el umbral de las propias fronteras de la red de la víctima y producir efectos (negativos) en la red de otro. Nunca se pueden sobrepasar los límites de la red de la organización y para tales acciones se debe solicitar el apoyo del organismo responsable.

2016 colocó en el panorama mundial la llamada Defensa Activa, actividades que pueden cruzar el umbral de las propias fronteras de la red de la víctima

MEDIDAS DE DEFENSA ACTIVA TENDENTES A BLOQUEAR UN CIBERATAQUE[46]



[46] Fuente: Center for Cyber & Homeland Security

INICIATIVAS INTERNACIONALES

Seguidamente, se muestran las iniciativas más significativas desarrolladas internacionalmente durante los últimos meses de 2015 y 2016.

- **Directiva Europea NIS**: en julio de 2016, el Parlamento Europeo adoptó la Directiva sobre seguridad de las redes y los sistemas de información que exige a todos los Estados disponer de capacidades propias en materia de ciberseguridad, fortaleciendo la cooperación entre estados y estableciendo requisitos específicos para los operadores de servicios esenciales. En España, se ha constituido un grupo de trabajo que está desarrollando la ley de transposición de dicha Directiva.

  Se establece la obligación de adoptar una estrategia nacional, con requisitos en materia de seguridad y noticiación, además de la designación de autoridades nacionales competentes. Asimismo se requerirán puntos de contacto únicos y CSIRT[47] con funciones relacionadas con la ciberseguridad.

- **Regulación General de Protección de Datos (RGPD)**: el pasado 4 de mayo de 2016, tras varios años de tramitación, se publicaron los instrumentos normativos que constituyen el nuevo marco europeo de protección de datos personales.

  - **Reglamento Europeo 2016/679, de 27 de abril**, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación.

  - **Directiva 2016/680, de 27 de abril**, relativa a la protección de las personas físicas respecto al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

  - **Directiva 2016/681, de 27 de abril**, relativa a la utilización de datos del registro de nombre de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

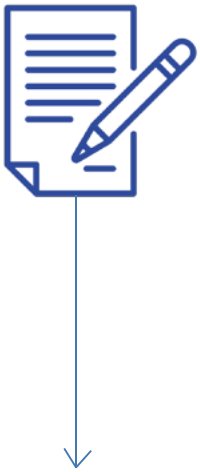
  Esta regulación basa la aplicación de las medidas de seguridad en el análisis de riesgos y de impacto. Se establecen como obligatorias / recomendables la aplicación de medidas basadas en códigos de buenas prácticas y esquemas de certificación y la notificación de incidentes.

- **Despliegue de CSIRT en el mundo**: se ha potenciado enormemente el desarrollo de las capacidades de respuestas en muchos países, teniendo la misión de apoyar a las organizaciones en la resolución de los ciberincidentes detectados. Hay cientos de CSIRT en el mundo, con distintas misiones y alcances. En 2016, el número de equipos adscritos a FIRST[48] era de 369, de 80 países distintos, entre ellos 14 de España.

- **Revelación responsable de vulnerabilidades de seguridad**: como mecanismo para conciliar la actividad de los ciberinvestigadores con la necesaria discreción de los hallazgos encontrados. En abril de 2016, la International Standardisation Organisation (ISO) publicó el documento ISO 29147 sobre revelación de vulnerabilidades.

En el informe de amenazas completo (CCN-CERT IA-16/17) se dispone de una relación de otras iniciativas llevadas a cabo por países de nuestro entorno.

Destaca el **Índice Mundial de Ciberseguridad** para comparar el nivel de ciberseguridad implantado, a partir de la iniciativa ***Global Cybersecurity Agenda*** de la **Unión Internacional de Telecomunicaciones** (ITU).



La Directiva Europea NIS exige a todos los Estados disponer de capacidades propias en materia de ciberseguridad

[47] Computer Security Incident Response Team. Equipo de respuesta ante ciberincidentes.
[48] Principal organización de CSIRT del mundo https://www.first.org

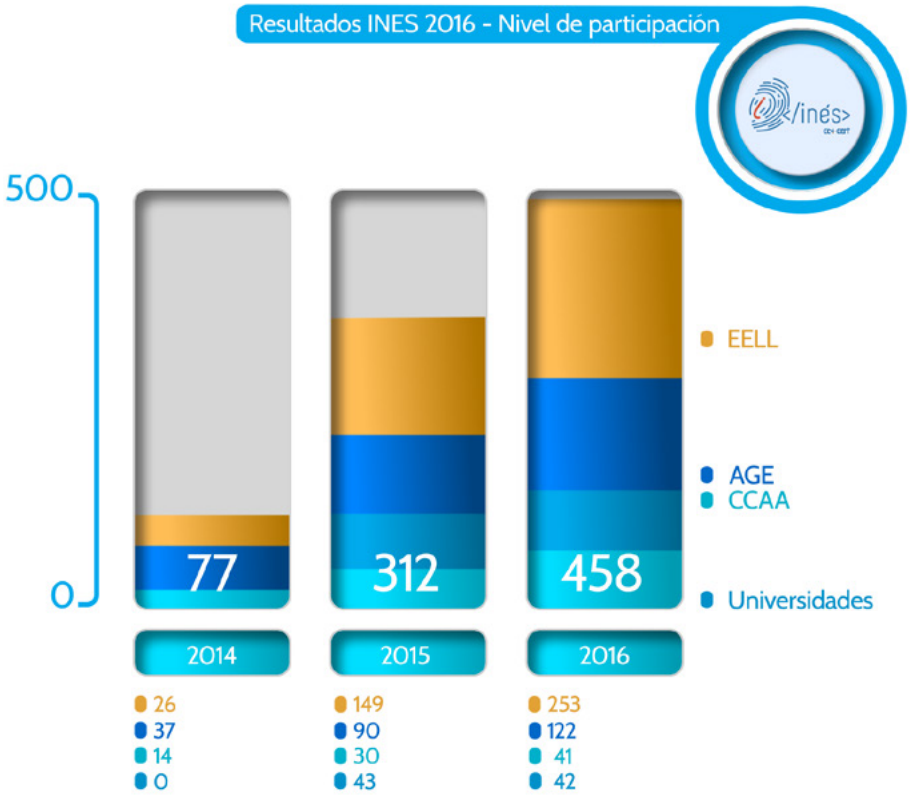
Iniciativas nacionales: el Esquema Nacional de Seguridad

El año 2016 ha sido especialmente importante para el desenvolvimiento electrónico de la actividad del Sector Público español.

- **La Ley 39/2015**, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de Régimen Jurídico del Sector Público, ambas de 1 de octubre de 2015 (entrada en vigor en noviembre de 2016).

- Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad (Resolución de 7 de octubre de 2016). El **Informe Nacional del Estado de la Seguridad** (INES) de los sistemas de las tecnologías de la información y la comunicación de 2016 ha incluido datos de 458 organismos del sector público, con un total de 14.577 sistemas TIC declarados que dan servicio a 3.467.434 usuarios y del que se obtiene una valoración global nacional del grado de implantación del Esquema Nacional de Seguridad.

- Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad (Resolución de 13 de octubre de 2016).



7 TENDENCIAS PARA 2017

¿HACIA DÓNDE VAMOS?

CIBERESPIONAJE

Se mantendrá muy activo en 2017, ya sea como parte de las operaciones de inteligencia de un Estado o dirigido por grupos organizados que proporcionarán servicios o buscarán información de interés y la podrán a la venta. Se prevén más acciones de influencia en procesos de decisión y de cibersabotaje en el marco de las operaciones híbridas.

NUEVOS TIPOS DE ATAQUES COMPLEJOS

Existen **mecanismos de infección sin utilizar malware**, ni escribir (casi) nada en disco desde hace muchos años. Cada vez va a ser más habitual el empleo de malware en **modo "sin archivos"** ejecutado en memoria y buscando su persistencia como **tarea programada** directamente desde el **registro.**

ELEMENTOS QUE CARACTERIZAN A LOS GRUPOS DE CIBERESPIONAJE MÁS "AVANZADOS"

- Uso de exploits de día-cero[49].
- Vectores de infección desconocidos, no identificados con anterioridad.
- Compromiso de varias organizaciones gubernamentales en varios países.
- Sustracción exitosa de información durante muchos años antes de ser descubiertos.
- Tener la capacidad de sustraer información de redes aisladas.
- Disponer de múltiples canales de exfiltración.
- Código dañino en la memoria de los equipos, sin utilizar el disco.
- Técnicas de persistencia avanzadas que utilizan funciones no documentadas.

Será necesario incrementar y ampliar las capacidades de vigilancia basadas en anomalías y mejorar el intercambio de patrones de detección en cualquier formato (IoC[50], reglas Yara, etc.).

[49] Exploit día cero: aprovechamiento de una vulnerabilidad inmediatamente después de haber sido descubierta, sin que sea públicamente conocida.
[50] Indicator of Compromise, Indicador de Compromiso.

MIENTRAS QUE LAS INFRAESTRUCTURAS CRÍTICAS Y LOS SISTEMAS DE CONTROL INDUSTRIAL CONTINÚEN CONECTADOS A INTERNET SIN LAS ACTUALIZACIONES NECESARIAS Y CON CONFIGURACIONES POR DEFECTO, CON POCA O NINGUNA PROTECCIÓN DE PERÍMETRO, SEGUIRÁN SIENDO OBJETIVO DE LOS ATACANTES

INFECCIONES EFÍMERAS

Se incrementará el uso de código dañino residente en memoria y destinado a reconocimiento general y recolección de credenciales, **sin persistir en el sistema de la víctima**. Esta nueva situación exige el concurso de nuevas y más sofisticadas herramientas de detección.

AMENAZAS AL HARDWARE Y FIRMWARE[51]

Las vulnerabilidades de hardware pueden socavar el funcionamiento y la seguridad de toda la pila de software. Así, la explotación de una vulnerabilidad de hardware puede comprometer todo un sistema y no requiere una explotación completa. Además, los sistemas cuyo hardware es atacado son difíciles de reparar.

DISPOSITIVOS MÓVILES COMO OBJETIVO DE CIBERESPIONAJE

Cada vez es más frecuente el uso de dispositivos móviles en ambientes profesionales, por lo que se espera que durante 2017 se incrementen las campañas de ciberespionaje dirigidas a estos equipos y, en concreto, el crecimiento del ransomware, troyanos bancarios y herramientas de monitorización y acceso remoto.

ATAQUES A ENTIDADES FINANCIERAS

Más que a sus usuarios. Es probable que 2017 sea testigo de un incremento de los ataques directamente contra las infraestructuras tecnológicas del sistema de pagos electrónico, así como la comercialización de estos ataques mediante servicios del tipo ***Crime-as-a-service***[52].

DESCONFIANZA EN EL RANSOMWARE

Estos ataques se basan en el principio de que el agresor respetará un contrato tácito con la víctima. Sin embargo, es muy posible que aparezcan casos en que a pesar de haber pagado el rescate no se desbloqueen los ficheros cifrados. Esto puede provocar una crisis de confianza que conduzca a pensar que "pagar el rescate" no conduce a nada, que de hecho es la recomendación del CCN-CERT. Sea como fuere, seguirá siendo una amenaza muy significativa en 2017, incluyendo el *Ransomware-as-a-Service*.

CIBERATAQUES CONTRA SISTEMAS DE CONTROL INDUSTRIAL

Mientras que las Infraestructuras Críticas y los sistemas de control industrial continúen conectados a Internet sin las actualizaciones necesarias y con configuraciones por defecto, con poca o ninguna protección de perímetro, seguirán siendo objetivo de los atacantes.

[51] Firmware funciona como el nexo de unión entre las instrucciones (software) que llegan al dispositivo desde el exterior y las diversas partes electrónicas (hardware).
[52] Cibercrimen como servicio.

COOPERACIÓN SEGURIDAD FÍSICA Y LÓGICA

Es presumible que en 2017 las industrias de la seguridad física y la ciberseguridad trabajen juntas para crear soluciones de seguridad integrales. Los proveedores de ciberseguridad comenzarán a prestar servicio y dar soporte a los proveedores de seguridad física ofreciendo nuevo software, plataformas y arquitecturas para la integración.

DÉBIL SEGURIDAD DEL INTERNET DE LAS COSAS

Mientras los fabricantes de dispositivos IoT[53] sigan produciendo dispositivos sin funcionalidades de seguridad, es probable que se aprovechen estas vulnerabilidades para perpetuar su control sobre dichos dispositivos. Esta situación podría dar como resultado la necesidad de desactivar los dispositivos vulnerables.

DRONEJACKING

Se han visto ejemplos de ataques empleando drones equipados con un conjunto de herramientas de ciberataque que les permitiría acceder a redes inalámbricas del objetivo.

REVELACIÓN DESCONTROLADA DE VULNERABILIDADES

Se han publicado en fuentes abiertas gran cantidad de exploits para múltiples tecnologías (Shadowbrokers, Vault 7,...) a los que siguieron múltiples ataques, con una paradoja subyacente: dispositivos creados para impedir la entrada del atacante, como firewalls, antivirus, IDS, etc. que posibilitan su penetración.

PRIVACIDAD

El seguimiento con cookies persistentes seguirá siendo un gran valor y es probable que en 2017 esta realidad se amplíe aún más combinada con widgets[54] que permitan a las compañías rastrear los hábitos de navegación de los usuarios.

PUBLICIDAD COMO HERRAMIENTA DE ATAQUE

Las redes publicitarias proporcionan perfiles muy completos de usuarios (direcciones IP, patrones de navegación e inicios de sesión). Este tipo de datos permite a un atacante discriminar o redirigir su código dañino a los objetivos deseados. Es de esperar, por lo tanto, que en 2017 atacantes avanzados consideren la creación/utilización de una red publicitaria para alcanzar sus objetivos.

REDEFINICIÓN DE LAS INVERSIONES EN TIC

Se invertirá más en aplicaciones móviles, migración a la nube y detección y respuesta a incidentes en los próximos ejercicios.

MIENTRAS LOS FABRICANTES DE DISPOSITIVOS IoT SIGAN PRODUCIENDO DISPOSITIVOS SIN FUNCIONALIDADES DE SEGURIDAD, ES PROBABLE QUE SE APROVECHEN ESTAS VULNERABILIDADES

[53] Internet of Things.
[54] Programa o aplicación similar a un acceso directo, pero además de acceder al programa determinado de forma rápida, también a funciones frecuentemente usadas y a diferente información visual. Por ejemplo, las de escritorio suelen ser aplicaciones para el tiempo, el reloj, buscadores, etc.

VULNERABILIDADES EN TECNOLOGÍAS

Se estima que el coste de vulnerabilidades día cero de las tecnologías Apple y Microsoft se incrementará considerablemente. Se espera durante 2017 una reutilización de las vulnerabilidades y herramientas publicadas en diferentes fuentes abiertas como Wikileaks.

APRENDIZAJE AUTOMÁTICO *(MACHINE LEARNING)* PARA ATAQUES DE INGENIERÍA SOCIAL

Con un impacto cada vez mayor en la educación, los negocios y la investigación, la disponibilidad de herramientas de aprendizaje automático (machine learning) ha reducido el período de aprendizaje y la accesibilidad para todos, incluidos los cibercriminales.

ATAQUE A LA PRIVACIDAD COMO HERRAMIENTA DEL CIBERACTIVISMO

En 2016 aumentó la concienciación de los usuarios sobre su "huella digital" y la necesidad de protegerla con la misma intensidad que en la vida real y seguirá aumentando en 2017. Pero, los ciberactivistas seguirán aprovechando el volumen de datos que el equipo del usuario recopila como información personal, búsquedas, enlaces, conexiones, visitas de páginas, uso de productos, etc. para exfiltrarlos a continuación, exhibiendo tales contenidos públicamente con diferentes finalidades.

Compartir la inteligencia de amenazas desplaza el equilibrio de poder de los adversarios a las víctimas, interrumpe el ciclo de vida de un ataque y resulta más costoso para los atacantes

PROGRESO DEL INTERCAMBIO DE INTELIGENCIA DE AMENAZAS

Compartir la inteligencia de amenazas desplaza el equilibrio de poder de los adversarios a las víctimas, al tiempo que interrumpe el ciclo de vida de un ataque y resulta más costoso para los agentes de la amenaza.


CCN-CERT
centro criptológico nacional
WWW.CCN-CERT.CNI.ES
WWW.OC.CCN.CNI.ES
WWW.CCN.CNI.ES
You Tube