Ciberamenazas y Tendencias
Edición 2017
CCN-CERT IA-16/17

Junio 2017

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 12:28:15 +02'00'

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como **CERT Gubernamental/Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a esta normativa, es competencia del CCN-CERT la gestión de ciberincidentes que afectan a sistemas del **sector público**, a **empresas y organizaciones de interés estratégico** para el país y a cualquier **sistema clasificado**. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. SOBRE EL PRESENTE INFORME

Buena parte de la información aquí recogida es el resultado de la experiencia del CCN-CERT durante 2016 en el desarrollo de sus competencias. Asimismo, se han tenido en cuenta otras fuentes documentales, nacionales e internacionales, públicas y privadas, y se ha contado con la colaboración de entidades externas, profesionales y miembros del mundo académico.

2.1 Contenido / Ámbito

Este documento contiene un análisis de las ciberamenazas, nacionales e internacionales, de su evolución y tendencias futuras, y ha sido realizado con el propósito de resultar de utilidad para los responsables de seguridad TIC de las entidades públicas españolas, las organizaciones de interés estratégico, así como a los profesionales y ciudadanos de nuestro país.

El ámbito del presente Informe es mundial, aunque se ha hecho más énfasis en los países de nuestro entorno europeo y occidental. Asimismo, en determinados epígrafes, se han realizado acotaciones específicas para España y los intereses españoles en el extranjero, con especial incidencia en las redes y sistemas de información de las entidades del Sector Público español y sus Infraestructuras Estratégicas.

2.2 Base documental

La información que ha servido de base para la confección del presente Informe proviene de diferentes fuentes: documentos internos del CCN y de sus organismos homólogos internacionales (especialmente, de la Unión Europea, EE.UU. y los socios y aliados de España), documentos públicos emanados de las unidades especializadas de los organismos públicos españoles, documentación de terceros (empresas y

organizaciones privadas) y, finalmente, estudios y trabajos de profesionales del sector privado y miembros de la Academia.

Para todos ellos, un año más, nuestro agradecimiento.

2.3 Clasificación y periodo de aplicación

El presente Informe se publica "SIN CLASIFICAR", no estando sujeto, por tanto, a las restricciones relativas a la información clasificada.

Los datos referidos a los "Ciberincidentes de 2016" comprenden el año natural 2016 incluyendo, en algún caso y para mejor comprensión de la evolución de los hechos citados, algún dato relativo al último semestre de 2015 y los primeros meses de 2017. El apartado "Tendencias para 2017", contiene algunas cuestiones que, en las materias citadas, será oportuno esperar en el presente año.

3. RESUMEN EJECUTIVO

A mediados de 2016, el número de usuarios de internet en todo el mundo era de más de tres mil millones y medio de personas, sobre un total estimado de más de siete mil millones de habitantes. Así pues, a efectos prácticos, la mitad de los habitantes de nuestro planeta ya son usuarios de internet.

La figura siguiente muestra el desglose de los usuarios mundiales de internet atendiendo a su ubicación geográfica[1].

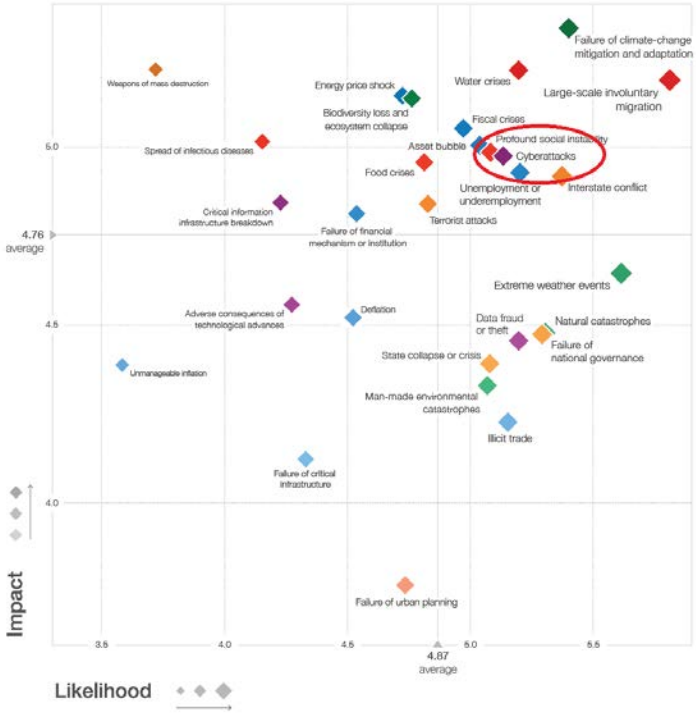
WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2016 - Update						
World Regions	Population (2016 Est.)	Population % of World	Internet Users 30 June 2016	Penetration Rate (% Pop.)	Growth 2000-2016	Table % Users
Asia	4,052,652,889	55.2 %	1,846,212,654	45.6 %	1,515.2%	50.2 %
Europe	832,073,224	11.3 %	614,979,903	73.9 %	485.2%	16.7 %
Latin America / Caribbean	626,119,788	8.5 %	384,751,302	61.5 %	2,029.4%	10.5 %
Africa	1,185,529,578	16.2 %	340,783,342	28.7 %	7,448.8%	9.3 %
North America	359,492,293	4.9 %	320,067,193	89.0 %	196.1%	8.7 %
Middle East	246,700,900	3.4 %	141,489,765	57.4 %	4,207.4%	3.8 %
Oceania / Australia	37,590,820	0.5 %	27,540,654	73.3 %	261.4%	0.8 %
WORLD TOTAL	7,340,159,492	100.0 %	3,675,824,813	50.1 %	918.3%	100.0 %

A medida que las innovaciones tecnológicas -tales como la economía compartida, *Blockchain* o el *Internet de las Cosas*-, se multiplican y penetran más profundamente en el mundo físico, es correlativamente más probable el aumento de los ciberriesgos. Por ejemplo: todos los datos apuntan a que el número de dispositivos conectados a Internet se triplicará en 2020, pasando de 13.400 millones a 38.500 millones, esperándose que la proporción de productos vendidos vía comercio electrónico aumente más del doble, del 6% en 2014 al 12.8% en 2019[2].

1 Fuente: Internet World Stats. (Véase: http://www.internetworldstats.com/stats.htm)

2 Fuente: World Economic Forum, "Understanding Systemic Cyber Risk", Octubre, 2016.

La figura siguiente muestra la relación impacto/probabilidad de los ciberataques, dentro de los riesgos globales considerados por el World Economic Forum[3]. Como puede observarse, el WEF sitúa a este riesgo entre los más significativos.



Desde luego, no todos los países del mundo están sujetos a los mismos riesgos ni han adoptado las mismas medidas de ciberseguridad. En 2015, la *International Telecommunications Organization (ITU)* publicó un informe en el que se incluían los países del mundo con mayor grado de confiabilidad sobre tales materias. Las primeras posiciones de la lista estaban ocupadas por Estados Unidos, Canadá, Australia, Malasia, Omán, Nueva Zelanda, Noruega, Brasil, Estonia, Alemania, India, Japón, República de Corea, Reino Unido, Austria, Hungría, Israel, Países Bajos, Singapur, Letonia, Suecia, Turquía, Hong Kong, Finlandia, Qatar, Eslovaquia, Uruguay, Colombia, Dinamarca, Egipto, Francia, Mauricio, España, Italia y Marruecos[4].

De forma análoga a lo que ha venido sucediendo en los últimos años, durante 2016 las más importantes amenazas para la ciberseguridad vinieron de la mano de los estados y las organizaciones delincuenciales[5].

Los siguientes han sido los elementos más significativos del entorno de la ciberseguridad mundial durante 2016.

3 Fuente: World Economic Forum, "The Global Risks Report 2016". 11Th edition. 2016.

4 Fuente: ITU: Índice Mundial de Ciberseguridad y Perfiles de Ciberbienestar. (2015). Se trata de la iniciativa lanzada por la Unión Internacional de Telecomunicaciones (ITU) denominada Agenda Mundial de Ciberseguridad (GCA), un marco de trabajo para la cooperación internacional que busca aumentar la confianza y seguridad en una sociedad de la información. La CGA tiene como base cinco "pilares estratégicos" también conocidos como "áreas de trabajo": medidas legales, medidas técnicas y de procedimiento, estructuras organizacionales, creación de capacidad y cooperación internacional. A partir de ellas surge el Índice Mundial de Ciberseguridad (GCI), que tiene como objetivo medir y evaluar el compromiso de los países en la materia.

5 Según Verizon (2016 Data Breach Investigations Report), el 86% de las brechas de seguridad persiguen motivos económicos o de espionaje.

- El **ciberespionaje de naturaleza económica**, llevado a cabo habitualmente por servicios de inteligencia extranjeros, ha constituido la mayor amenaza para el mundo occidental en el último año, dirigiéndose, fundamentalmente, contra organizaciones, públicas y privadas, poseedoras de importantes activos en materia de propiedad intelectual.
- El **ciberespionaje de naturaleza política**, llevado a cabo, igualmente, por estados extranjeros, ha pretendido socavar el contexto político y gubernamental de los estados atacados, persiguiendo, en muchos casos, atentar contra el orden legal constituido. En ocasiones, además, se han podido observar acciones de cibersabotaje cómo medidas de apoyo a acciones militares convencionales.
- La **ciberdelincuencia**, que se ha centrado en buena medida en el desarrollo de redes de ordenadores infectados (botnets), proporcionar servicios de ataque y en el despliegue masivo de campañas de ransomware, cada vez más organizadas. Así, por primera vez, hemos visto cómo este tipo de ataques ha tenido en cuenta la capacidad económica de las víctimas, solicitando un rescate mayor si mayores eran los recursos económicos de las entidades atacadas. El incremento en su sofisticación, la utilización de correos electrónicos dirigidos (spear-phising) y el crecimiento en el número de tales ataques constituyen las novedades más significativas de esta actividad delincuencial.
- El **cifrado de la información**, como mecanismo más idóneo para garantizar la confidencialidad, ha sido una de las tecnologías más estudiadas y controvertidas. Durante 2016 ha resurgido con especial intensidad el debate entre el uso de los procedimientos criptográficos por parte de los usuarios y la posibilidad de los gobiernos por disponer de elementos -tecnológicos, pero también jurídicos- que permitan el acceso a la información cifrada, cuando se posea evidencia de acciones delictivas. Una vez más, nos hemos encontrado ante el permanente debate entre seguridad y libertad. Mientras que en algunos estados han podido promulgarse normas legales facilitando el acceso a información cifrada bajo ciertas circunstancias[6], en otros, sin embargo, la garantía del secreto de las comunicaciones ha prevalecido sobre de los deseos de las agencias gubernamentales y sus fuerzas de seguridad[7].
- El **ciberactivismo**, pese a constituir a día de hoy una amenaza de menor calado que la ciberdelincuencia organizada y el ciberespionaje estatal, sigue estando presente y aunque no han podido constatarse ataques graves desarrollados por estos actores, su impacto en el mundo mediático ha sido especialmente significativo. Estos grupos han centrado sus acciones en la publicación de información, tanto corporativa como personal.

6 Tal es el caso, por ejemplo, de las recientes normas aprobadas en Alemania, Francia y el Reino Unido.

7 Como ha sido el caso, por ejemplo, de los Países Bajos.

- La amenaza de los **cibervándalos** y **script kiddies** sigue en aumento, como lo demuestra el significativo incremento de ataques DDoS desarrollados con herramientas muy accesibles y de bajo coste, entre las que se incluye el *Cibercrimen-as-a-Service* del que ya hemos dado cuenta en anteriores ediciones de este informe. La presencia de exploits-kits, contando en muchos casos con servicios de ayuda disponibles 24/7, y el aumento de código dañino para dispositivos móviles, junto con una significativa facilidad de uso, han provocado que estos actores, marginales hasta hace unos años, se han transformado en especialmente peligrosos.
- Los **ataques DDoS** han seguido en aumento. Llevados a cabo, fundamentalmente, por cibercriminales, ciberactivistas, cibervándalos y script kiddies, han perseguido, además de hacer caer los sistemas afectados, propiciar el uso de la extorsión, amenazando con provocar ataques DDoS a aquellas instituciones que no se plegaban al chantaje. Aunque han sido muchas las organizaciones que, durante 2016, han tomado medidas -individuales o colectivas- para hacer frente a los ataques DDoS, muchas otras no han podido acometerlas debido al coste que supone su implantación.
- Puede observarse un **déficit en las pequeñas y medianas organizaciones**, tanto del sector público como del privado, en la adopción de medidas de seguridad tendentes a minimizar los efectos de los ciberincidentes, lo que, dado su significativo número, representa una significativa repercusión.
- La **actualización del software** de los equipos y dispositivos continúa siendo un reto. En muchas ocasiones, la vulnerabilidad de las organizaciones está provocada por la existencia de equipos o dispositivos que albergan software desactualizado o que no han incorporado adecuadamente los parches de seguridad.
- El crecimiento de la **publicidad dañina** en páginas web muy conocidas y visitadas ha provocado un incremento inusitado en la distribución de código dañino a través de anuncios, aumentando la superficie de ataque y generando un grave riesgo para los visitantes de tales páginas. En muchas ocasiones la solución no contempla por eliminar la publicidad de tales páginas, puesto que tendría un impacto muy negativo en el modelo de negocio de muchas empresas.
- El **comportamiento de los usuarios** sigue constituyendo una de las más importantes vulnerabilidades de los sistemas, propiciando que la ingeniería social siga siendo uno de los mecanismos más usados para iniciar ciberataques, a través, generalmente, de spear-phishing.

El cuadro de la figura siguiente esquematiza los agentes de las amenazas más significativos durante 2016, la tipología de sus acciones y sus víctimas[8].

8 Fuente: Cyber Security Assessment Netherlands. CSAN 2016 y elaboración propia.

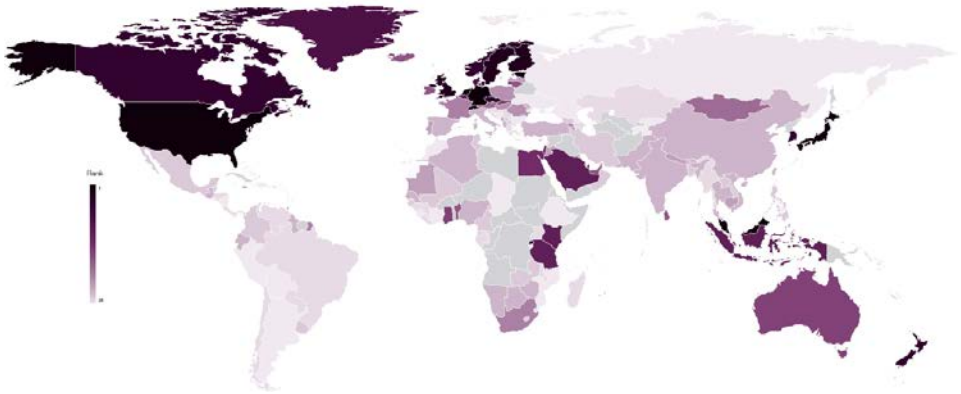
	Víctimas		
Agentes de las amenazas	**Sector Público**	**Organizaciones privadas**	**Ciudadanos**
Estados	Ciberespionaje político	Ciberespionaje económico	Ciberespionaje
	Capacidades ofensivas	Capacidades ofensivas	
Organizaciones criminales	Robo y publicación o venta de información	Robo y publicación o venta de información	Robo y publicación o venta de información
	Manipulación de la información	Manipulación de la información	Manipulación de la información
	Disrupción de sistemas	Disrupción de sistemas	Disrupción de sistemas
	Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas
Organizaciones privadas		Ciberespionaje industrial o económico	Abuso o reventa de información corporativa
Ciberterroristas	Disrupción / toma de control de sistemas	Disrupción / toma de control de sistemas	
Ciberyihadistas	Propaganda / Reclutamiento	Propaganda / Reclutamiento	Propaganda / Reclutamiento
Ciberactivismo	Robo y publicación de información	Robo y publicación de información	
	Desfiguraciones	Desfiguraciones	
	Disrupción de sistemas	Disrupción de sistemas	
	Toma de control de sistemas	Toma de control de sistemas	
Civervándalos y script kiddies	Robo de información	Robo de información	Robo de información
	Disrupción de sistemas	Disrupción de sistemas	
Actores internos	Robo y publicación o venta de información	Robo y publicación o venta de información	
	Disrupción de sistemas	Disrupción de sistemas	
Ciber-investigadores	Publicación de información	Publicación de información	

Código de colores:	No han aparecido nuevas amenazas. o Existen suficientes medidas para eliminar la amenaza o No han existido incidentes apreciables derivados de la amenaza.	Se han observado nuevas tendencias o fenómenos asociados con la amenaza. o Existe un conjunto de medidas limitadas para eliminar la amenaza o El número de incidentes derivados de la amenaza no ha sido especialmente significativo	Existen claros desarrollos relacionados con la amenaza o Las medidas desplegadas tienen un efecto limitado en la amenaza o El número de incidentes derivados de la amenaza ha sido significativo

El cuadro siguiente resume el nivel de riesgo global percibido, según datos del World Economic Forum[9], en las 140 economías cubiertas por el estudio.

Riesgo	Porcentaje
Desempleo o Subempleo	41
Explosión de los precios de la energía	29
Fallo de la gobernabilidad nacional	14
Burbuja de activos	11
Crisis fiscal	10
Ciberataques	8

La figura siguiente muestra el riesgo de ciberataques percibido por distintas regiones mundiales[10].



4. LOS CIBERINCIDENTES DE 2016

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

9 World Economic Forum: "Global Risks Report 2016"

10 WEF, Op. Cit.

4.1 Ciberespionaje

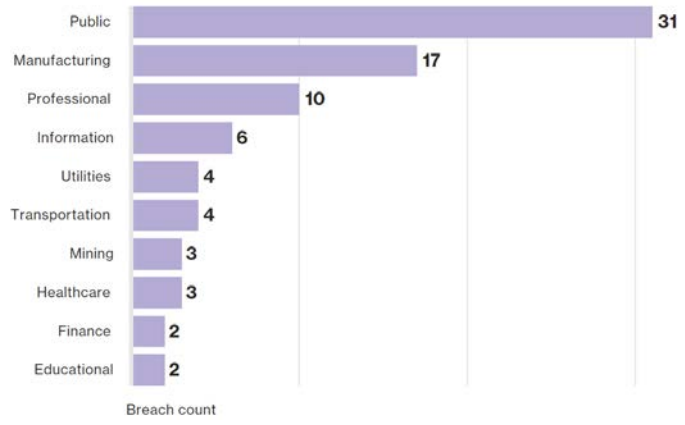
Para España -como para el resto de los países occidentales- el ciberespionaje sigue constituyendo la mayor amenaza para la seguridad nacional. Durante 2016, los servicios de inteligencia occidentales han observado un importante crecimiento del **ciberespionaje económico**, especialmente dirigido a las industrias de los sectores de la Defensa, Alta Tecnología, Industria Química, Energía y Salud, persiguiendo en la mayor parte de los casos el acceso a desarrollos avanzados.

Este tipo de ataques, en cuyo origen hay que colocar a ciertos estados y empresas extranjeras, están provocando alteraciones en el orden económico mundial por lo que tienen de elementos perturbadores de la competencia, sin entrar a considerar ahora otras posibles consecuencias, tales como la utilización de la información indebidamente obtenida para incrementar el arsenal armamentístico de los estados atacantes.

De la sofisticación con la que se realizan estos ataques se deriva la dificultad de su detección, que puede demorarse semanas, meses e, incluso, años[11].

Por su parte, el **ciberespionaje político**, con origen en los servicios de inteligencia extranjeros, sigue constituyendo una de las principales amenazas para la seguridad internacional. Europa y España no son una excepción: durante 2016 se han detectado multitud de ataques de este tipo que han perseguido obtener información de naturaleza política, económica o estratégica, así como planes de desarrollo y posiciones nacionales en torno a debates o negociaciones abiertas.

La figura siguiente muestra los sectores-víctima más usuales de los ataques de ciberespionaje.



Aunque en menor medida, conviene señalar también los ataques que ciertas minorías étnicas han sufrido durante 2016, fácilmente atribuibles a los gobiernos de sus países de origen.

11 Según un artículo publicado por la revista Volkskrant, en junio de 2016, la empresa Rheinmetall, especializada en sistemas para la defensa, había estado siendo víctima de un ataque con posible origen chino desde 2012, habiendo sido descubierto al final de 2015 por la empresa de seguridad Fox-IT.

4.2 La delincuencia en el ciberespacio

Las más recientes estimaciones de Europol, señalan que, en 2016, se ha producido un aumento sustancial de las acciones delincuenciales en el ciberespacio, lo que ha provocado que, en determinados países de la Unión Europea, el ciberdelito podría haber superado a la delincuencia tradicional en términos de denuncia[12]. Algunos ataques, como los provocados por **ransomware** -que, además, han evidenciado un mayor grado de agresividad- se han convertido en algo habitual, eclipsando las amenazas tradicionales de código dañino, tales como los troyanos bancarios.

Por su parte, el ya maduro modelo **Crime-as-a-Service** continúa proporcionando herramientas y servicios en todo el espectro de los actores cibercriminales, desde los principiantes hasta las organizaciones más profesionalizadas.

En Europa, la utilización de la tecnología EMV (chip y PIN), el llamado geoblocking y otras medidas han conseguido limitar los fraudes en la utilización de **tarjetas bancarias**, forzando a los ciberdelincuentes a migrar sus acciones a otras regiones. Sin embargo, ataques contra los Terminales Punto de Venta continúan proliferando y en plena evolución. En 2016, por ejemplo, se han observado las primeras acciones realizadas por grupos organizados dirigidas a tarjetas NFC.

Como señalábamos en nuestro Informe del pasado año, los **ataques DDoS** continúan creciendo en intensidad y complejidad (mezclando, en ocasiones, ataques en las capas de red y de aplicación). Las herramientas para su perpetración, como los denominados booters/stressers[13], fácilmente disponibles *as-a-service*, han propiciado el incremento de tales ataques. Por otro lado, mientras que ciertos tipos de ataques persiguen exfiltrar credenciales bancarias, existe una tendencia creciente en lograr el comprometimiento de otros tipos de datos, tales como datos médicos y otros datos sensibles o relativos a propiedad intelectual.

El creciente uso delincuencial de **servicios y herramientas de anonimización y cifrado** plantea un serio problema para la detección, investigación y enjuiciamiento, comportando una amenaza especialmente significativa, que toca todas las áreas del delito. El cifrado es muy importante para el comercio electrónico y otras actividades en el ciberespacio, pero, como suele señalarse desde los Cuerpos Policiales, la seguridad adecuada depende de que tales instituciones posean la capacidad de investigar la actividad delictiva.

Ransomware y Cryptoware

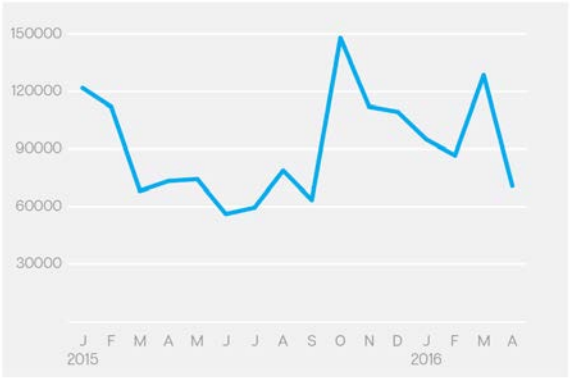
Sin duda alguna, el **ransomware** ha sido el vector de ataque que más ha crecido durante 2016. El número de infecciones por ransomware ha aumentado en todo el mundo de manera exponencial, destaca su empleo en el sector de la energía (persiguiendo la disrupción de los sistemas). Por su parte, los sectores gubernamentales,

12 Fuente: Europol: IOCTA, 2016. (Véanse: Office for National Statistics, Crime in England and Wales: year ending Mar 2016, https://www.gov.uk/government/statistics/crime-in-england-and-wales-year-ending-mar-2016 y NCA Strategic Cyber Industry Group Cyber Crime, Cyber Crime Assessment 2016, http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

13 Booters/stressers son herramientas para realizar pruebas de stress a los servidores, que podrían ser mal utilizados para realizar ataques DDoS.

sanitario y de telecomunicaciones también han tenido que hacer frente a un extraordinario incremento del número de acciones de este tipo.

La figura siguiente muestra las infecciones mundiales por ransomware, en el periodo considerado, atendiendo a un estudio de Symantec[14].



En España, el CCN-CERT gestionó un total de 2.030 incidentes de distintos tipos de ransomware (un 375% más que en 2015) y elaboró sendos Informes de Buenas Prácticas[15] y de Amenazas [16] sobre este tipo de ataque (al tiempo que analizaba algunos de los tipos más comunes en sus Informes de Código Dañino[17])

Ransomware	Incidentes
Cryptowall	278
Torrentlocker	308
Locky	785
Critroni	72
Teslacrypt	319
Cryptolocker	151
BandarChor	7
FileCoder	2
Cerber	59
Radamant	48
CryptXXX	1

Considerando la tipología de los ataques, una de las conclusiones más importantes que pueden obtenerse es que el modo de infección por ransomware está cambiando: los ataques se están volviendo más dirigidos, como lo demuestra el hecho de que una

14 Symantec: Special Report: Ransomware and Businesses, 2016.

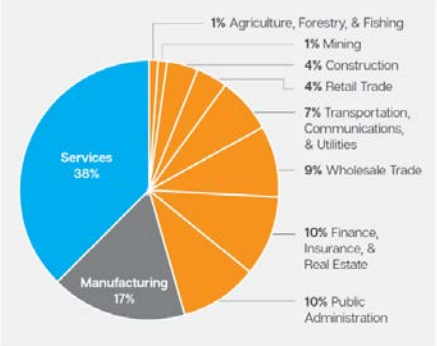
15 CCN-CERT BP-04/16 https://www.ccn-cert.cni.es/informes/informes-ccn-cert-buenas-practicas-bp/2088-ccn-cert-bp-04-16-ransomware/file.html

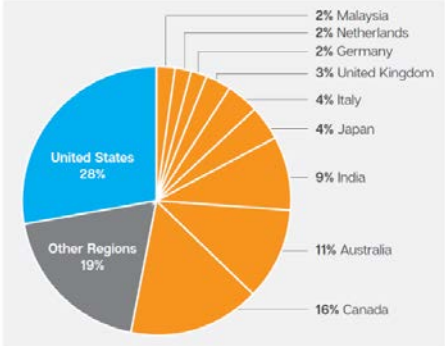
16 CCN-CERT IA-03/17 https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1974-ccn-cert-ia-03-17-medidas-seguridad-ransomware-1/file.html

17 Bart, VenusLocker, Petya, Satana, Locky, CryptXXX, Cerber, DMALocker, Mischa, CryptoWall y TeslaCrypt fueron analizados en los Informes de Código Dañino de 2016 del CCN-CERT https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html?limit=25&limitstart=25

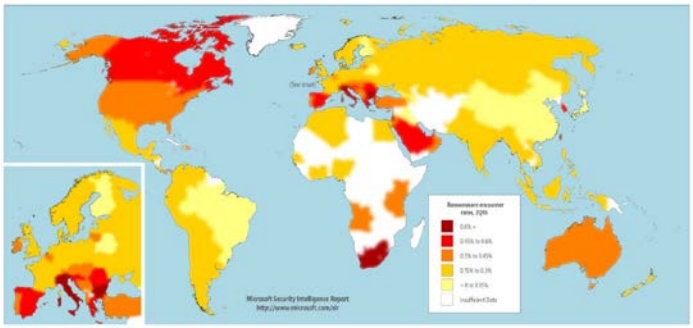
buena parte de los que fueron víctimas indicaron que tuvieron su origen a través de mecanismos de ingeniería social, especialmente mediante el uso de correos electrónicos dirigidos, en algún caso, a las cuentas de correo privadas de directivos de las entidades atacadas.

Como decimos, y así se muestra en la figura de la izquierda, los sectores más atacados fueron los Servicios, la Fabricación y el Sector Público. Como en otros tipos de infecciones, el ransomware ataca a las entidades de los países más desarrollados, como muestra la figura de la derecha, de la misma fuente.





Atendiendo a datos suministrados por Microsoft, sobre detección de ransomware en ordenadores con base en el sistema operativo del fabricante, la figura siguiente muestra el impacto mundial de este tipo de código dañino en el segundo semestre de 2016. Obsérvese la alta incidencia registrada en España[18].



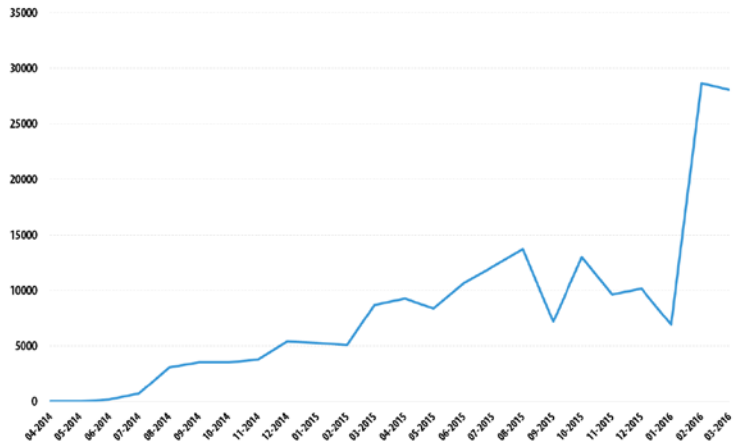
18 Fuente: Microsoft Security Intelligence Report Volume 21 | January through June, 2016.

Además de esta característica, durante 2016 la sofisticación del ransomware también ha afectado a los sistemas de Back-up, haciendo imposible en muchos casos su recuperación. Como decimos, un sector especialmente delicado ha sido el sector sanitario, que ha sufrido importantes ataques de ransomware durante 2016[19].

En el cuadro siguiente se muestran tres muestras de ransomware más frecuentemente detectadas en 2016.

Cerber	**CryptXXX**	**Locky**
Nombre de la detección: Trojan.Cryptolocker.AH Cuantía extorsión: 1.24 to 2.48 BTC (de $513 a $1,026, en cifras de marzo de 2016) Descubrimiento: Marzo, 2016 Vectores de infección: Campañas de spam, exploit kit Neutrino, exploit kit Magnitude	Nombre de la detección: Trojan.Cryptolocker.AN Cuantía extorsión: $500 en bitcoin Descubrimiento: Abril, 2016 Vectores de infección: exploit kit Angler, exploit kit Neutrino	Nombre de la detección: Trojan.Cryptolocker.AF Cuantía extorsión: 0.5 a 1 bitcoin (de $200 a $400, en cifras de febrero de 2016) Descubrimiento: Febrero, 2016 Vectores de infección: Campañas de spam, exploit kit Neutrino, exploit kit Nuclear

Finalmente, el ransomware también ha atacado a los dispositivos móviles. La figura siguiente muestra lo espectacular de su crecimiento en los últimos dos años, evaluado en número de usuarios con dispositivos comprometidos[20].



Publicidad dañina

2016 ha sido un año especialmente significativo en ciberincidentes provocados por la presencia de publicidad dañina en páginas web muy conocidas de todo el mundo. En

19 Un par de ejemplos: en febrero de 2016, un hospital de la ciudad alemana de Neuss fue víctima de un ataque de Ransomware que cifró la información de los pacientes. La página de noticias alemana RP Online señaló que cinco grandes hospitales alemanes sufrieron el mismo tipo de ataque. Por su parte, el Presbyterian Medical Center de Los Ángeles también fue víctima de un ciberataque por Ransomware en esas mismas fechas, provocando la caída de los sistemas que controlaban los equipos TAC, robos de laboratorio y sistemas de expedición de medicamentos. Según se afirma, el hospital pagó un rescate de 17.000 dólares. http://venturebeat.com/2016/02/17/los-angeles-hospital-paid-hackers-17000-ransom-in-bitcoins/

20 Fuente: Kaspersky Lb: Corporate IT Security Risks Special Report Series 2016: the cost of cryptomalware: SMBS at gunpoint. (Encuesta realizada a más de 3.000 responsables de Pymes, en todo el mundo).

muchas ocasiones, la metodología seguida por los atacantes sugiere la presencia de ciberdelincuentes[21].

Pese a que un modo de evitar este problema es la instalación de software anti-publicidad, el modelo económico de rentabilidad de algunas páginas web se vería afectado de manera significativa, lo que hace imposible, por el momento.

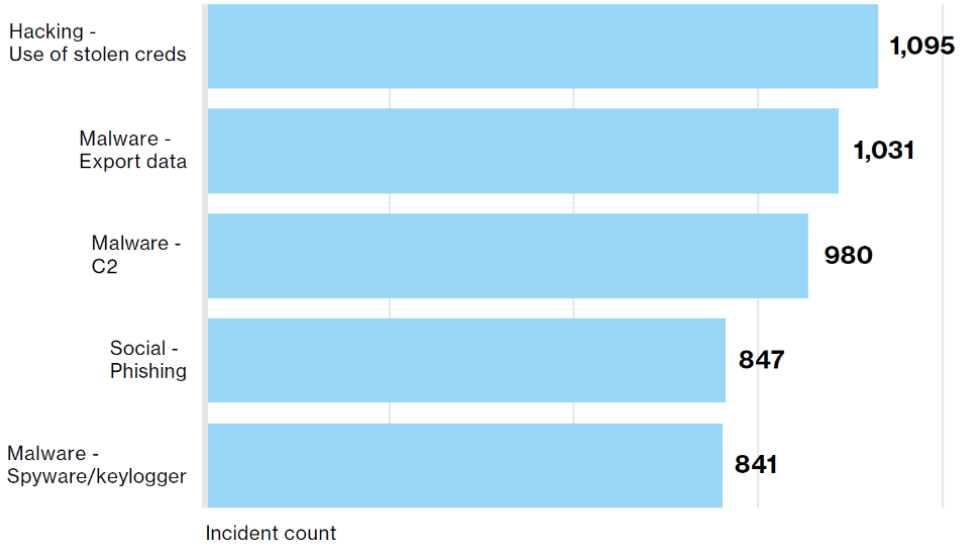
Los ataques a las entidades financieras

Aunque las entidades financieras han sufrido menos acciones dañinas dirigidas a usuarios finales, los ataques por ransomware y RAT (Remote Access Tools) continúan aumentando, dirigidos especialmente a las propias entidades[22].

Estas últimas herramientas (RAT) gozan de un especial predicamento entre los agentes de las amenazas, puesto que, pese a la complejidad de su despliegue, permiten investigar las redes de las víctimas y detectar dónde se encuentran los activos de valor. Además de ello, han aparecido lugares donde se pueden contratar estas actividades en modo servicio.

No obstante lo anterior, siguen observándose campañas de phishing en las que se requiere a los usuarios para que suministren información personal asociada a sus cuentas (tales como credenciales, por ejemplo)[23].

La figura siguiente muestra las principales variedades de amenazas dentro de los incidentes relacionados con la sustracción de credenciales[24].



Los foros underground contienen multitud de ejemplos de venta de credenciales sustraídas. El cuadro siguiente muestra una tabla de los precios habituales[25].

21 Por ejemplo, en abril de 2016, la empresa Fox-IT detectó una campaña de publicidad dañina que afectó al menos a 288 páginas web de los Países Bajos. Los atacantes usaron el exploit-kit Angler para infectar a los usuarios con código dañino.

22 Como se observó en los ataques Carnabak, en que los atacantes si dirigieron contra transacciones desarrolladas a través de la red internacional Swift.

23 Un ejemplo: en noviembre de 2015, un atacante que se hizo pasar por la Agencia de Cobros Judicial de los Países Bajos (CJIB), instó a que pagaran lo antes posible sus cuentas pendientes, cosa que muchos hicieron, creyendo que las transferencias iban dirigidas a la entidad real y no al ciberdelincuente.

24 Fuente: Verizon "2016 Data Breach Investigations".

Offering	Price
Origin account access	Less than US$1
Spotify account access	US$2
Beats Music account access	US$2
Hulu Plus account access	US$4
Netflix account access	US$5
Dish Network Anywhere account access	US$7
Luminosity account access	US$7
Verified PayPal account access	US$9
Sirius Satellite Radio account access	US$15

El phishing sigue siendo uno de los vectores de ataque más significativos, habiéndose experimentado un incremento notable en cuanto a la dificultad para distinguir un mensaje dañino de otro real[26], así como la determinación, cada vez más precisa, de las víctimas[27]. Todo esto hace que el nivel de éxito de estos ataques sea significativamente alto[28].

Sustracción de información

Muchos han sido los ejemplos recientes de sustracción de información (muchas veces, de naturaleza personal) derivados de ataques dirigidos a instituciones concretas. Así, los centros hospitalarios han visto cómo el número de tales ataques se incrementaba significativamente (originándose a través de phishing, habitualmente), y en el que los atacantes han perseguido, con propósitos económicos, la obtención de las credenciales de acceso de las víctimas. En otros casos, los objetivos perseguidos por los atacantes han servido para desarrollar acciones de contra-espionaje o para presionar a los gobiernos con chantajes[29].

25 Fuente: TrendMicro: North America Underground.

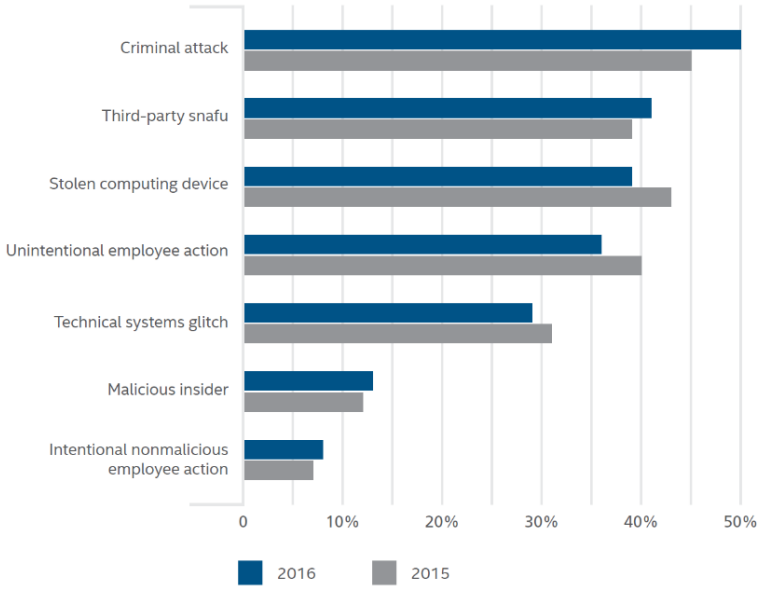
26 Como cuando el atacante se hace pasar por un directivo de la entidad, ataque conocido como CEO fraud.

27 Como cuando los ataques se dirigen, expresamente, a miembros del departamento IT de la entidad, al objeto de obtener información relevante sobre la infraestructura tecnológica de la organización.

28 Por ejemplo, en febrero de 2016, se sustrajeron 81 millones de dólares del Banco Central de Bangladesh, a través de un acceso fraudulento a transacciones Swift. (http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0XI1UO). Este ataque se intentó con anterioridad contra el Tien Phong Bank de Vietnam. (http://www.reuters.com/article/us-vietnam-cybercrime-idUSKCN0Y60EN) y, posteriormente, contra el Banco del Austro de Ecuador. (http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD)

29 Tales fueron los casos, por ejemplo, de los 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 (https://www.opm.gov/cybersecurity/cybersecurity-incidents/), 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, en el que sus autores amenazaron con hacer públicos los nombres de los usuarios si no se cerraba el portal, cosa que, finalmente, sucedió. (http://nos.nl/op3/artikel/2052728-hackers-zetten-32-miljoen-vreemdgangers-online.html. Es muy posible que otros ciberdelincuentes usarán la información publicada para hacer chantaje a las personas comprometidas con la filtración (http://www.zdnet.be/nieuws/171086/hackers-chanteren-ashley-madison-gebruikers/) y que pudieran haber sido causantes de algunos suicidios (http://www.volkskrant.nl/buitenland/-twee-zelfmoorden-na-hack-ashley-madison~a4128352/)

Atendiendo a un estudio internacional, la figura siguiente muestra las causas originarias de la fuga de información en las instituciones sanitarias[30].



El robo de información también ha afectado a formaciones políticas[31] y a gobiernos de países occidentales[32].

En Europa, datos de Europol señalan que industrias como la hostelería y el comercio representan un porcentaje significativo de las brechas de datos[33]. Además, los intercambiadores de divisas virtuales, así como los operadores de estas plataformas son asimismo objetivos particularmente atractivos para los ciberataques. Algunos informes indican que hasta el 89% de las brechas de datos tienen un motivo financiero o de espionaje[34].

El cuadro de la figura siguiente muestra las más significativas brechas de seguridad en 2016[35].

30 Fuente: Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2016, Ponemon Institute.

31 Tales como el Partido Demócrata norteamericano, que en junio de 2016, fue víctima de un ataque, -en un principio atribuido a actores rusos y más tarde a un desconocido personaje- cuyos autores se apropiaron de correos electrónicos y mensajes de distintos usuarios del partido.
(http://nos.nl/artikel/2111102-russische-hackers-maken-data-democraten-buit.html)
(http://www.darkreading.com/attacks-breaches/russian-hackers-breach-democrats-to-steal-data-on-trump/d/d-id/1325909)

32 En Agosto de 2016, un grupo autodenominado Shadow Brokers, manifestaron que se habían introducido en una campaña de ciberespionaje de los EE.UU., sustrayendo un código dañino -parte del cual hicieron público- que posibilitaba tales acciones. Otra parte de lo sustraído se intentó vender en pública subasta.
(http://www.nu.nl/internet/4307673/hackersgroep-claimt-nsa-spionagesoftware-hebben-gestolen.html)

33 Fuente: Europol – IOCTA, 2016.

34 Fuente: Europol, op. cit.

35 Fuente: Breach Level Index, Data Breach Statistics, (véase: http://www.breachlevelindex.com/#!breach-database)

ORGANISATION	INDUSTRY	COUNTRY	SOURCE OF BREACH	RECORDS COMPROMISED	DATA COMPROMISED
Fling	Adult		Malicious outsider	40 000 000	Email address, passwords, IP address, date of birth, sexual preferences
T Mobile	Telecoms		Malicious insider	1 500 000	Undisclosed
Kiddicare	Retail		Malicious outsider	794 000	Name, address, email address, telephone number
Nulled.io	Criminal		Unknown	474 000	Username, email address, IP address, hashed password, personal messages
Kinoptic	Technology		Accidental loss	198 000	Username, email address, hashed password
Rosebutt Board	Adult		Malicious outsider	107 000	Username, email address, IP address, hashed passwords
Postbank, Commerzbank, and Landesbank Berlin	Finance		Malicious outsider	85 000	Credit card data
Swiss People's Party (SVP)	Government		Malicious outsider	50 000	Name, email address
Islamic State Human Resources & Recruiting	Military		Malicious insider	22 000	Name, address, telephone number, place of birth and sponsor
University of Greenwich	Education		Malicious outsider	21 000	Name, address, date of birth, telephone number, signature
Engitel	Technology		Hacktivist	20 000+	Username, email address
Faithless	Entertainment		Malicious outsider	18 000	Email address
National Childbirth Trust (NCT)	Other		Malicious outsider	15 000	Email address, username, password
ShOping.su	Criminal		Malicious outsider	16 500	Username, email address, compromised card details
University of Liverpool	Education		Malicious outsider	6 500	Name, address, email address

Métodos de monetización

Aunque hay un sinnúmero de tipologías distintas de datos que pueden sustraerse y, en su consecuencia, muchas formas de monetizar tal sustracción, estas son las que han sido más frecuentes en 2016.

- Información de tarjetas bancarias: beneficios directos.

- Información de las cuentas bancarias: exfiltración de dinero, troyanos bancarios[36].
- Información personal: robo de identidad, chantaje, etc.

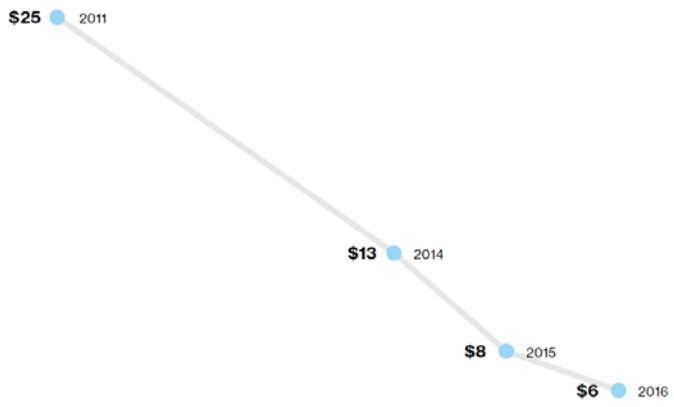
Pese a que, con frecuencia, también suele sustraerse otro tipo de información (tal como la relativa a la propiedad intelectual o mecanismos de acceso a sistemas de información) estos datos no suelen "ponerse a la venta" puesto que, en muchas ocasiones, suele ser más valioso su conocimiento que su comercialización.

En una publicación de McAfee Labs de otoño de 2015[37], se identificaron los siguientes precios como precios de venta promedio de las tarjetas robadas:

Payment Card Number With CVV2	United States	United Kingdom	Canada	Australia	European Union
Random	$5–$8	$20–$25	$20–$25	$21–$25	$25–$30
With Bank ID Number	$15	$25	$25	$25	$30
With Date of Birth	$15	$30	$30	$30	$35
With Fullzinfo	$30	$35	$40	$40	$45

Estimated per card prices, in US$, for stolen payment card data (Visa, MasterCard, Amex, Discover).

Como quiera que existen numerosas opciones de compra y, en su consecuencia, resulta difícil establecer tendencias de mercado a lo largo del tiempo, seguidamente se muestra un gráfico que refleja los cambios en los precios de una tarjeta de pago robada en los Estados Unidos[38].

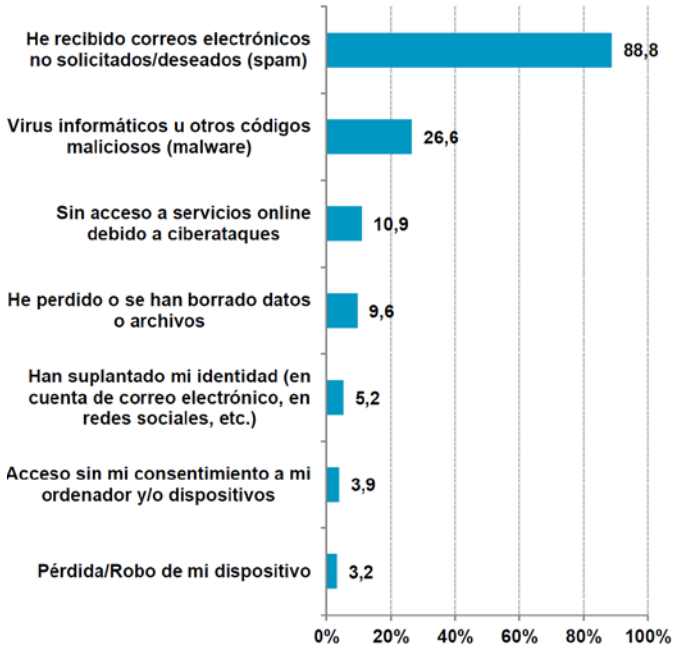


36 Por ejemplo, Zeus, Dyre y Dridex.

37 The Hiden Data Economy (véase: http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf)

38 Fuente: Intel Security. Precios en dólares US.

Por lo que respecta a los ciudadanos españoles, la figura siguiente muestra el porcentaje de usuarios particulares que han sufrido alguna incidencia de seguridad en 2016[39].



4.3 Disrupción de sistemas

Ataques DDoS

Durante 2016, muchas organizaciones de todo el mundo han sido víctimas de ataques DDoS. Aunque es posible adoptar medidas efectivas contra este tipo de ataques, tales medidas son costosas. Además de hacer caer los sistemas de las víctimas, cada vez es más frecuente que el motivo de los ataques esconda una extorsión: se insta a las víctimas a pagar un rescate a cambio de no iniciar un ataque DDoS[40].

Sabotaje digital

Aunque el mayor peligro (siempre latente) es el ataque con origen en estados extranjeros[41], hasta el momento los ataques que han puesto en riesgo las infraestructuras esenciales se han originado en exempleados descontentos que han seguido utilizando sus credenciales de acceso para causar daños a sus antiguas organizaciones, considerables en ocasiones. Pese a lo anterior, se observa que muchos estados están incrementando el uso de herramientas que desde el ciberespacio apoyen alcanzar sus objetivos tácticos o estratégicos[42].

39 Fuente: ONTSI: Estudio sobre la Ciberseguridad y confianza en los hogares españoles (Nov., 2016)

40 Un ejemplo de organización para la extorsión en base a amenazas DDoS es el grupo llamado DD4BC (DDoS for bitcoin).

41 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.

42 Algunos ejemplos de esta tendencia pueden observarse en los conflictos de Ucrania y Siria, donde tales herramientas se utilizan regularmente.

Desfiguraciones

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

Infraestructuras Críticas

El cuadro siguiente muestra los ataques más significativos reportados en Infraestructuras Críticas, ya sean operadas por el sector público o el privado, desglosando el vector de ataque[43].

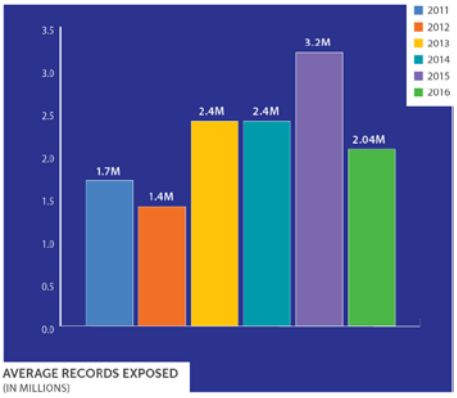
		Number of studies per sector									
Nr.	Attack / Threat	Public Administration	Energy	Health	Financial	ICTs	Transport	Water	Aerospace	Food	Chemistry
1	Malware	7	10	7	9	9	7	1	1	1	1
2	DoS/DDoS	10	8	8	11	11	8	1	1	1	–
3	Cyber Espionage	2	3	3	3	2	1	1	1	–	1
4	Web-Based Attacks	5	7	4	7	7	6	–	1	1	–
5	Insider Threat	7	4	6	8	7	3	–	1	1	–
6	Hacktivism	3	3	3	5	4	–	–	1	1	1
7	Malicious Code	5	6	5	7	7	6	–	–	–	–
8	Phishing	6	4	4	6	6	4	1	–	–	–
9	Web Application Attacks	5	2	4	4	4	2	1	–	–	–
10	Ransomware	3	1	3	2	2	1	1	–	–	–
11	Botnets	1	2	2	2	2	2	–	–	–	–
12	Critical Vulnerabilities	1	1	1	–	–	1	1	–	–	–

4.4 Los costes de los ciberincidentes y de su gestión

Es indudable que las brechas de seguridad tienen un coste global, derivado de varios costes parciales: económicos directos, de servicio, de reputación e imagen, por sanciones, etc. La figura siguiente muestra los costes derivados de los ciberataques, reportados a las compañías aseguradoras norteamericanas, en relación con las pérdidas sufridas por brechas de datos y otros tipos de ciberincidentes[44]. El 68% de las reclamaciones aportaron datos del número de registros comprometidos, que osciló entre 1 y 78 millones. La media de registros comprometidos fue de 2,04 millones.

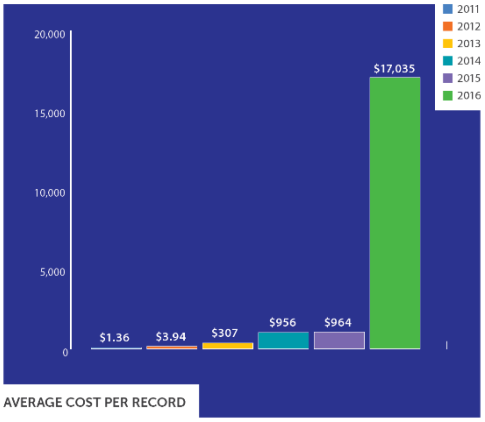
43 Fuente: ENISA: The cost of incidents affecting CIIs. Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII) (Agosto, 2016)

44 Fuente: Net Dilligence: 2016 Cyber Claim Study, sobre 176 expedientes de reclamaciones presentadas en 2016. De esta cantidad, 163 reclamaciones se referían a pérdida, exposición o mal uso de algún tipo de datos personales confidenciales. Los restantes 13 incidentes involucraron interrupción de negocios, sustracción pérdida de hardware perdido y ataques DDoS.



Las brechas de seguridad pueden involucrar muchos tipos de datos y, en su consecuencia, acarrear distintos costes, que pueden oscilar entre unos pocos cientos de dólares y cientos de millones de dólares[45], siendo el coste por registro comprometido independientemente del tamaño de la brecha.

La figura siguiente da una idea de los costes por registro comprometido. En el caso estudiado, el 66% de las victimas dieron datos sobre el número de registros comprometidos y el coste total de la brecha. Los costes mínimos/máximos por registro comprometido fueron de 0,03 dólares/1.6 millones de dólares. El coste medio por registro se situó en 17 dólares



Sólo en los Estados Unidos y en 2015, el *Internet Crime Complaint Center* (IC3) del FBI, gestionó 288.012 denuncias individuales que estimaron las pérdidas directas debidas a ciberincidentes en Internet en aproximadamente 1.070 millones de dólares[46]. La cifra de pérdidas en todo el mundo se cifra en torno a los 400.000 millones de dólares[47].

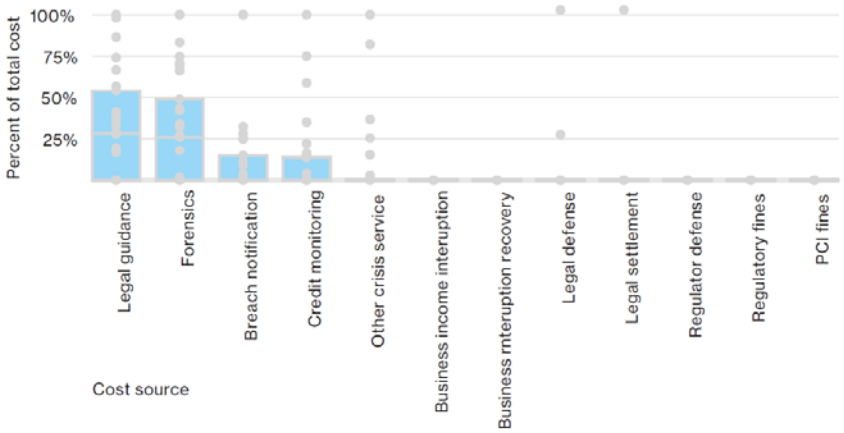
Una vez que se ha producido una brecha de seguridad y se es consciente de ello, el tratamiento del ciberincidente lleva implícito determinados costes que no conviene olvidar. Atendiendo a un estudio realizado por la empresa Verizon[48], la figura siguiente muestra el reparto de tales costes, atendiendo a las acciones que será necesario acometer. El asesoramiento legal durante la fase de gestión de crisis y las investigaciones forenses son, por lo general, las más costosas, seguidas por la notificación de violación y el mantenimiento de la imagen ante los clientes.

45 Un ejemplo: La brecha de seguridad Target ocasionó costes por valor de 250 millones de dólares.

46 Fuente: FBI-IC3: 2015 Internet Crime Report.

47 Fuente: Khoo Boon Hui (Ex presidente de INTERPOL). "Los cibercriminales se lucran en Internet". Fundación Innovación Bankinter – Fundación Future Trends Forum.

48 Verizon: "2016 Data Breach Investigations Report".



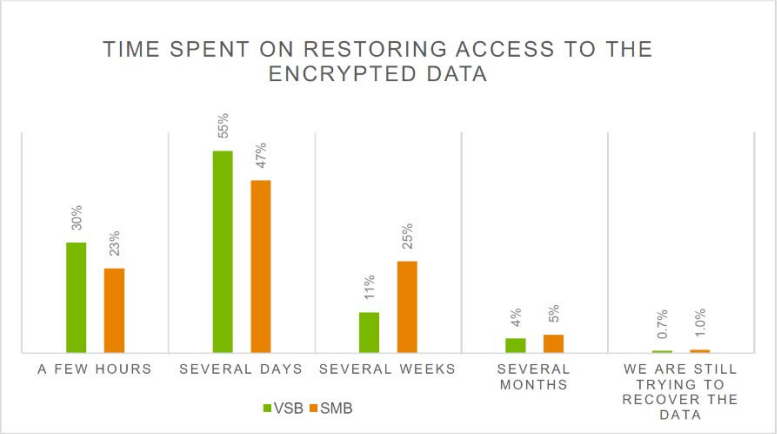
Por lo que respecta al ransomware, el rescate promedio exigido por los atacantes aumentó en 2016, elevándose a 679 dólares, frente a los 294 dólares de 2015. En 2016 también se registró un nuevo récord en términos de cuantía de la extorsión, con la amenaza conocida como Cryptolocker, que solicitó un rescate de 13 bitcoin por ordenador infectado (5.083 dólares, en el momento del descubrimiento, en enero de 2016)[49].

Pero el económico no es el único coste asociado al ransomware. El cuadro siguiente muestran los costes más significativos:

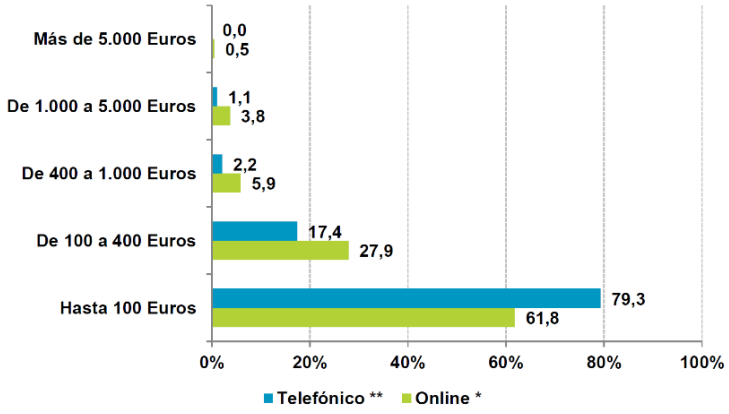
Costes de tiempo de inactividad: Las organizaciones atacadas pueden verse obligadas a cerrar sistemas para hacer frente a la infección. Los clientes, por tanto, se verán afectados. Debido a este tiempo de inactividad, la organización podría experimentar pérdidas económicas y daños reputacionales. En el caso de empresas de servicios públicos, la falta de energía o de agua podría afectar a millones de personas.	**Costes económicos**: Las empresas deben hacer frente a costes derivados de la respuesta a incidentes. Además, las organizaciones atacadas podrían también tener que hacer frente a responsabilidad económica frente a sus clientes e, incluso, al pago de cuantiosas sanciones por motivos legales.
Pérdida de datos: La pérdida de datos debido a que los archivos están cifrados y / o robados puede tener un enorme impacto en las empresas. La pérdida de los registros de la empresa, la información personal identificable de los clientes (PII) o la propiedad intelectual pueden afectar significativamente las finanzas, la marca y la reputación de la organización. Además, los ciberdelincuentes pueden amenazar con publicar datos robados, en un intento de obtener más dinero de la víctima.	**Pérdida de vidas**: En el caso de un hospital u otra organización médica, la vida de los pacientes puede ponerse en riesgo, ya que el equipamiento médico esencial podría verse afectado. Los registros de los pacientes, incluyendo la historia clínica, también pueden quedar inaccesibles, lo que provocaría retrasos en el tratamiento o, incluso, la prescripción de medicamentos incorrectos.

49 Fuente: Symantec: Special Report: Ransomware and Businesses, 2016.

El cuadro siguiente muestra el tiempo medio usado por las victimas para restaurar (cuando ello fue posible) los datos cifrados a su estado original[50].



Por lo que respecta a los ciudadanos españoles que han tenido un perjuicio económico debido a ciberincidentes, el gráfico siguiente muestra el reparto de tales costes[51].



5. AGENTES DE LA AMENAZA

Los últimos años han evidenciado que las amenazas a los sistemas de información, entendidas como *aquellos eventos que pueden desencadenar un incidente en las organizaciones, produciendo daños materiales o pérdidas inmateriales en sus activos*[52], siguen creciendo, y lo hacen tanto en tipología, en volumen como en sofisticación y, por consiguiente, en peligrosidad.

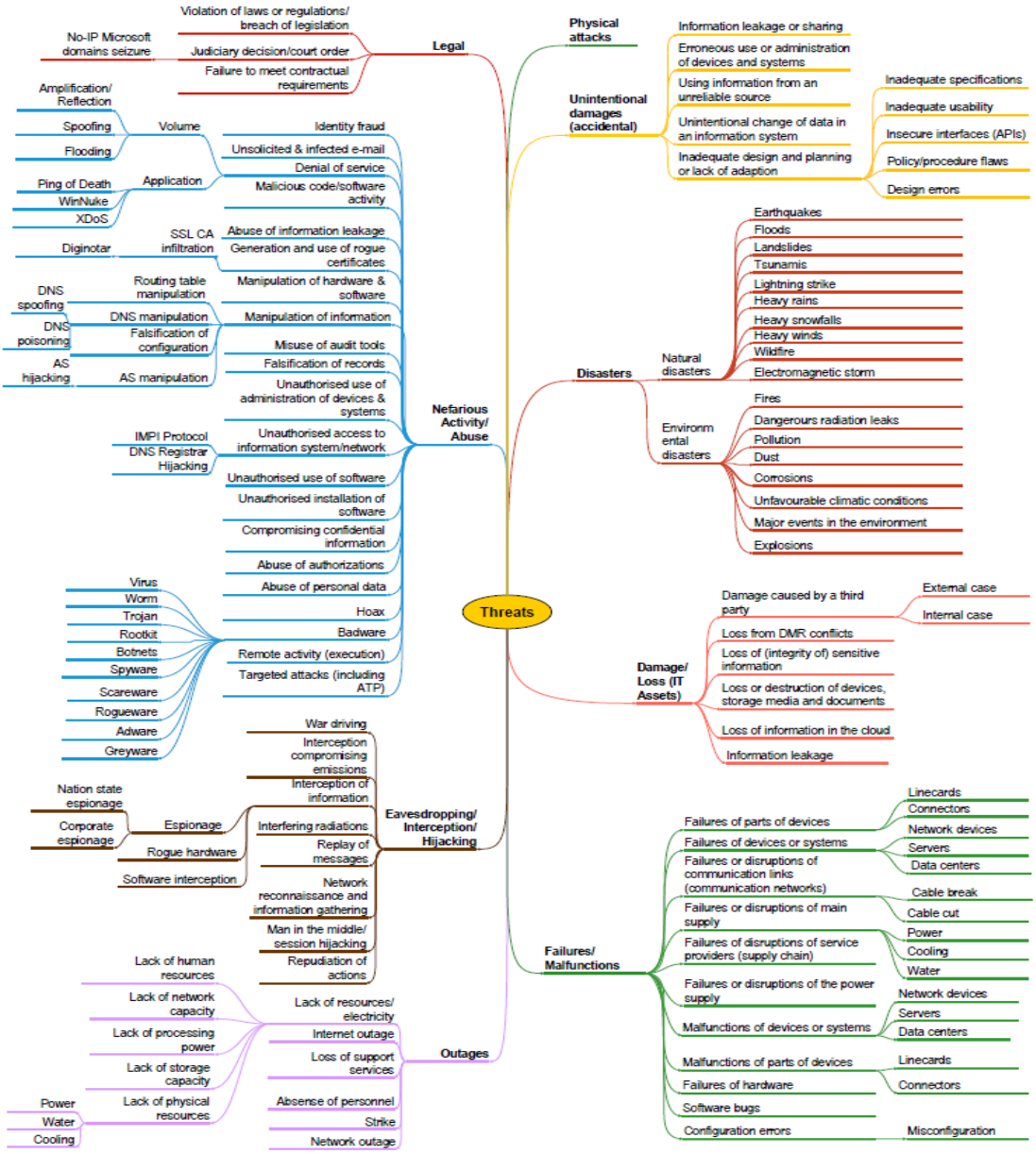
La figura siguiente muestra una taxonomía de las amenazas más frecuentes a los sistemas de información[53].

50 Fuente: Kaspersky Lb: Corporate IT Security Risks Special Report Series 2016: the cost of cryptomalware: smbs at gunpoint. (Encuesta realizada a más de 3.000 responsables de Pymes, en todo el mundo).

51 Fuente: ONTSI. Estudio sobre la Ciberseguridad y la confianza en los hogares españoles (Nov, 2016).

52 Fuente: Guía CCN-STIC 800 Esquema Nacional de Seguridad. Glosario de Términos y Abreviaturas. (Febrero, 2016)

53 Fuente: ENISA Threat Taxonomy. A tool for structuring threat information. (Jan., 2016)



En 2016 los estados y las organizaciones delincuenciales -cuyos vectores de ataque son análogos a los utilizados en los pasados años- constituyeron la mayor amenaza para las sociedades occidentales y la seguridad nacional. Los actores más significativos se tratan en este epígrafe.

5.1 Los Estados como agentes de las amenazas

Como hemos mencionado, la mayor amenaza para la ciberseguridad nacional lo constituyen las acciones de los estados, muy especialmente aquellas que tienen su origen en los Servicios de Inteligencia.

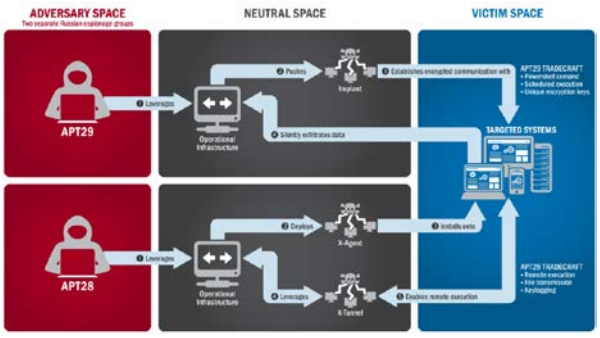
En general, las motivaciones habituales que persiguen los estados atacantes son las siguientes:

- Buscar información sobre los planes militares del estado atacado;
- Sustraer la propiedad intelectual y la inteligencia sobre las capacidades militares del estado atacado;
- Explotar las capacidades militares del estado atacado utilizando sus recursos militares y de inteligencia, conociendo las vulnerabilidades del estado atacado;
- Negar el uso del estado atacado de sus canales de comunicación en el ciberespacio;
- Realizar actividades subversivas[54] utilizando sus servicios de inteligencia; y
- Utilizar proxies o un gran número de elementos externos para cubrir el verdadero origen de sus actividades dentro del ciberespacio.

Un ejemplo: en el verano de 2015, un grupo conocido como APT29, sospechoso de trabajar para el gobierno ruso, consiguió penetrar en las redes del partido demócrata de los Estados Unidos. El vector de ataque fue mandar mensajes de correo con un enlace dañino a un millar de personas, entre ellas miembros del gobierno.

Ciertas webs de instituciones educativas y gubernamentales, con alguna vulnerabilidad conocida por los atacantes ayudaron a los atacantes, ya fuera como dominios desde los que mandar supuestos mensajes, o bien como sitios web donde albergar código dañino que infectarían a quien abriese el documento adjunto. Así, a través de esta puerta de entrada, se instaló código dañino en las redes del partido demócrata, logrando su control. Un año después, en primavera de 2016, otro grupo de atacantes -denominado APT28- usó la misma táctica para introducirse en el mismo partido político y exfiltró información de múltiples miembros, remitiendo tal información a la prensa.

La figura siguiente muestra el esquema de este ataque, que, a la fecha de redacción del presente Informe, ya ha provocado la salida de decenas de representantes diplomáticos rusos de los EE.UU.[55].



54 Otro ejemplo: la sustracción de datos personales de la Oficina de Administración de Personal de los Estados Unidos muestra el supuesto uso de operaciones cibernéticas por parte de un estado.

55 Fuente: NCCIC-FBI: GRIZZLY STEPPE – Russian Malicious Cyber Activity. Reference Number: JAR-16-20296 December 29, 2016.

Los ciberataques se han convertido en una alternativa real a las herramientas convencionales de inteligencia, muy especialmente debido a su bajo coste, a la dificultad de probar su autoría y al importante volumen de información que puede ser obtenido por esta vía. La mayor diferencia con relación a años pasados ha sido el incremento en los recursos en búsqueda de vulnerabilidades desconocidas y el aumento de la seguridad en estas operaciones.

El cuadro de la figura siguiente resume los ataques con posible origen china más significativos en el primer cuatrimestre de 2016[56].

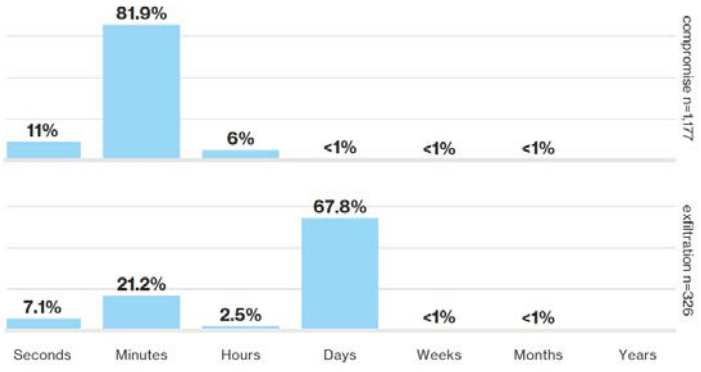
April – May 2016		Three groups compromised the networks of four firms headquartered in the U.S., Europe, and Asia that are involved in the manufacturing of semiconductors and chemical components used in the production of semiconductors. We did not observe data theft in any of these instances. However, in 2012, we saw one of these same groups compromise a semiconductor firm and target the workstation of a key individual active in research and development. Other China-based groups have also compromised and stolen data from semiconductor firms in the past, including as recently as July 2015.
April – May 2016		After compromising a network, the group moved laterally, harvested credentials, and deployed backdoors on systems at a U.S. high-tech corporation.
March – May 2016		In what appeared to be an attempt to obtain information related to U.S. military projects, a group deployed backdoors to a victim's web servers and harvested credentials at a U.S. government services company.
August 2015 – March 2016		After compromising the network of a U.S. high-tech corporation, the group began collecting data about navigational software in RAR files, likely in preparation for transferring the data from the environment.
March 2016		A group compromised a U.S. healthcare organization and deployed a backdoor providing continued access to the network.
December 2012-March 2016		In December 2012 a group breached the network of a U.S. software company. In 2014, they returned to the network, packaged data on navigational projects in likely preparation for removing it from the network. The same group returned again in early 2016 and viewed files related to the same project, but they did not transfer any data out of the network.
October 2015 – February 2016		In early 2016, a group prepared to transfer files out of the network of a European consulting company. The files were related to technology used in U.S. military projects.
January 2016		At a European logistics company a group collected user credentials during an intrusion into the network.

56 Fuente: FireEye, op. cit.

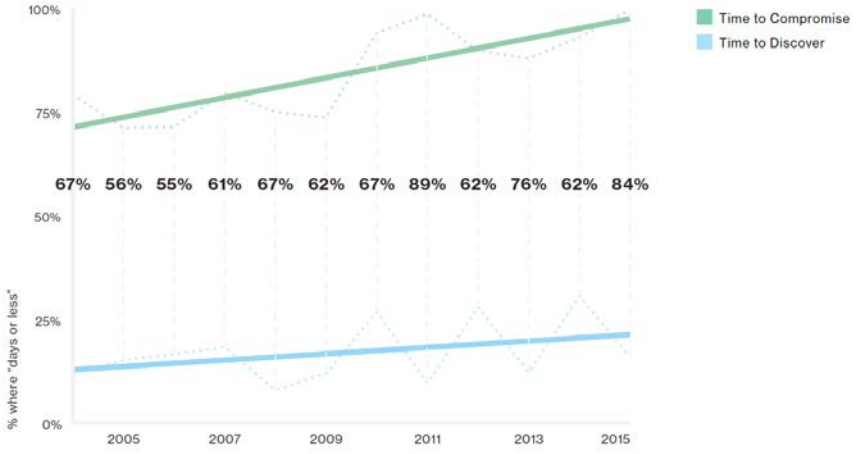
España ha recibido ataques especialmente dirigidos a las industrias de la Defensa, compañías Tecnológicas y entidades significadas del Sector Público.

Por otro lado, los estados siguen invirtiendo en el desarrollo de capacidades ciberofensivas, realizadas generalmente a través de los Servicios de Inteligencia. Existen evidencias de que ciertos estados han puesto en práctica tales capacidades en apoyo de sus intereses estratégicos o persiguiendo influir en conflictos nacionales o internacionales, así como, en ciertas ocasiones, apoyar sus intervenciones armadas, como herramientas complementarias a las tradicionales.

La figura siguiente, atendiendo a los datos revelados por Verizon, muestra el tiempo habitual requerido para lograr el compromiso de los sistemas atacados y la exfiltración de datos[57].



Del mismo estudio, la figura siguiente muestra -una vez más- la dificultad de descubrir un ataque, especialmente cuando se trata de un ataque dirigido.



5.2 Organizaciones delincuenciales

El crimen organizado en el ciberespacio tiene un enorme impacto tanto en los ciudadanos, como en las empresas o en las organizaciones del sector público.

57 Fuente: Verizon, "2016 Data Breach Investigations Report".

En general, tras los ataques de este tipo de actores se encuentra el deseo de obtener un beneficio económico directo (sustracción de credenciales) o indirecto (a través de extorsiones). Los mecanismos usados durante 2016 no han sido muy diferentes de los registrados en pasados años, advirtiéndose, eso sí, un importante incremento en la organización interna y en la mayor precisión de los ataques. Por primera vez nos hemos encontrado con ataques "persistentes", es decir, con la pretensión de mantenerse activos durante largos periodos de tiempo, incrementando los beneficios económicos de sus acciones.

En 2016 los ciberdelincuentes han puesto el foco en la extorsión digital, constituyendo el ransomware la prueba más evidente, incrementando notablemente su grado de sofisticación y apuntando con sus acciones a víctimas de las que previamente saben que pueden satisfacer el rescate solicitado[58], así como a ciertos objetivos de los que se sabe no pueden prescindir de sus sistemas de información, tales como servicios sanitarios[59] [60].

Otro vector de ataque han sido las campañas de extorsión, amenazando con provocar ataques DDoS si la víctima no satisfacía una cierta cantidad de dinero, generalmente usando criptomonedas. Los atacantes más conocidos en este sentido han sido DD4BC[61] y Armada Collective[62].

Finalmente, la extorsión ha alcanzado tanto a víctimas individuales cuyos datos o informaciones personales habrían sido previamente sustraídos de servicios web, como a organizaciones, donde los atacantes amenazaban con difundir información corporativa obtenida de ataques previos[63] si no se satisfacían sus exigencias.

El incremento de los ataques ha sido posible, en ciertas ocasiones, porque, se han hecho público muestras el código dañino, lo que ha facilitado su modificación y adaptación a los objetivos que pretendían atacar.

Como en años anteriores, el nivel de conocimientos de los ciberdelincuentes es muy variado, yendo desde los especialistas (caracterizados por un alto nivel de profesionalidad y de capacidad innovadora) hasta grupos de bajo nivel. Esta realidad ha provocado que la utilización del *Cybercrime-as-a-service* siga incrementándose, alcanzando también al que podríamos denominar *Ramsomware-as-a-service*[64], cuyos mecanismos de ataque han podido aparecer en YouTube y los códigos en GitHub.

58 Véase: http://arstechnica.com/security/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/
http://blog.trendmicro.com/trendlabs-security-intelligence/businesses-held-for-ransom-torrentlocker-and-cryptowall-change-tactics/

59 Véase: https://www.technologyreview.com/s/600838/hollywood-hospitals-run-in-with-ransomware-is-part-of-an-alarming-trend-in-cybercrime/
http://arstechnica.com/security/2016/03/kentucky-hospital-hit-by-ransomware-attack/

60 Tal fue el caso, por ejemplo, de un hospital norteamericano que pagó a los delincuentes 40 bitcoins (17.000 dólares) para que volvieron a dejar operativos los sistemas afectados, lo que incluía los datos de los pacientes y cierto tipo de equipamiento o médico. Véase:
https://www.security.nl/posting/461521/Amerikaans+ziekenhuis+betaalt+17_000+dollar+aan+ransomware

61 Véase: http://www.computerweekly.com/news/4500246707/DD4B-cyber-extortion-gang-targets-key-European-sectors
https://blogs.akamai.com/2015/05/dd4bc-escalates-attacks.html

62 https://blogs.akamai.com/2015/11/operation-profile-armada-collective.html

63 Véase: http://tweakers.net/nieuws/104536/hackers-zetten-inloggegevens-van-bitdefender-klanten-online.html
http://tweakers.net/nieuws/104290/rex-mundi-heeft-financiele-gegevens-duizenden-belgen-buitgemaakt.html

64 http://arstechnica.com/security/2016/01/researchers-uncover-javascript-based-ransomware-as-service/

Frente a todo ello, los procedimientos de identificación de los autores siguen siendo manifiestamente insuficientes. El uso de técnicas de anonimización dificultan extraordinariamente las labores investigadoras (empleo de proxies y redes Tor). Todo ello, unido al anonimato que se deriva del uso de criptomonedas, dificulta el seguimiento y la identificación de los autores. Además, se han detectado sistemas de cambio ilegal de Bitcoin, totalmente anónimos, que, pese al porcentaje que exigen de cada cambio (entre el 8 y el 12%, frente al 0,5% de los legales) están teniendo un notable éxito.

Finalmente, se ha observado un importante crecimiento en la cooperación (presencial, incluso) entre distintos grupos delincuenciales, aunando esfuerzos en la planificación y desarrollo de acciones conjuntas[65].

El crecimiento del *Cybercrime-as-a-service*

Esta actividad delincuencial, que ya hemos mencionado en anteriores ediciones, ha venido perfeccionándose en 2016, acomodando sus servicios a víctimas concretas y haciendo posible la cooperación de distintos grupos de delincuentes. La utilización de la Deep-web sigue siendo el lugar más frecuente para el intercambio de herramientas y la planificación de ataques[66].

Últimamente, se observan servicios ofrecidos bajo esta modalidad que contemplaban la venta de código dañino listo para su uso, información robada relativa a tarjetas de crédito, cuentas de correo electrónico y redes sociales, herramientas para el desarrollo de ataques DDoS o RAT especializados para la comisión de acciones delictivas.

La fiabilidad de tales prestadores ha venido incrementándose a lo largo de los años, incluyéndose, últimamente, la posibilidad de contratar un soporte de asistencia a los usuarios[67]. En algunos casos, además, se han observado comportamientos comerciales de los prestadores que animan a pagar a los clientes sólo cuando tengan éxito en sus acciones[68], o cuando el código dañino se instala correctamente (caso del exploit-kit Angler, por ejemplo[69]), contratando una suscripción o haciendo accesible el código dañino durante un determinado período de tiempo (caso de exploit-kit Sweet Orange, por ejemplo[70]).

En otros casos, se han observado condiciones por parte del prestador del servicio para usar el código dañino, tales como comprometerse a usar la herramienta sólo en ataques dirigidos o en determinados países, incluyendo en algunos casos, la participación de los beneficios obtenidos.

5.3 El terrorismo en el ciberespacio

Por el momento, siguen sin apreciarse acciones terroristas en el ciberespacio, sin que ello signifique que no se haya observado un incremento en actividades, a escala reducida, relacionadas con grupos u organizaciones terroristas, para las que se usaron herramientas digitales. La mayor parte de estas acciones tuvieron su origen en lo que hemos denominado grupos Ciberyihadistas[71], sin que se hayan evidenciado ataques a gran escala o especialmente sofisticados.

65 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

66 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

67 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

68 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

69 https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

70 http://www.drchaos.com/sweet-orange-web-exploit-kit/

71 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).

La actividad del ciberyihadismo, además de provocar desfiguraciones de páginas web[72], pequeños ataques DDoS o contra cuentas de redes sociales, se ha concentrado en ocultar la información intercambiada a través de canales de comunicación cifrados. Asimismo, durante 2016 han aparecido nuevos foros yihadistas en el ciberespacio[73] con objetivo de difundir sus mensajes, realización de propaganda y reclutamiento de nuevos elementos terroristas[74].

Aunque ciertos grupos terroristas han podido manifestar en 2016 que han desarrollado acciones que han tenido como resultado la obtención de información confidencial, lo cierto es que en la mayoría de los casos examinados la información pretendidamente sustraída podía localizar se públicamente en internet, para lo que solamente era necesario disponer de una limitada capacidad y recursos[75] [76].

Pese a todo, conviene hacer notar que los grupos yihadistas disponen de los medios económicos para perpetrar ciberataques a mayor escala. La capacidad tecnológica y los conocimientos precisos siguen siendo, sin embargo, sus puntos débiles, que están intentando solucionar contratando o atrayendo a la causa especialistas cuyo conocimiento pudiera permitirles la perpetración de ataques a mayor escala. Las denominaciones "Caliphate Cyber Army"[77] e "Islamic CyberArmy"[78] suelen aparecer habitualmente, en relación con ciberataques[79].

5.4 El ciberactivismo

Como quiera que la tecnología es capaz de amplificar la insatisfacción, los movimientos sociales ven facilitada su penetración usando herramientas digitales que permiten que el ciudadano sea escuchado como la movilización rápida de masas, el ciberactivismo y el desarrollo de movimientos sociales globalmente conectados, más allá de fronteras geográficas o políticas[80].

Como es sabido, estos grupos justifican sus acciones en base a motivos ideológicos, tan diversos como las capacidades que poseen. Durante 2016, las acciones

72 Como las que pudieron observarse tras los atentados de París.

73 Véase: http://www.nytimes.com/2016/01/15/world/middleeast/a-news-agency-with-scoops-directly-from-isis-and-a-veneer-of-objectivity.html?_r=0
http://www.mirror.co.uk/news/technology-science/technology/hidden-isis-android-app-lets-6203483
http://securityaffairs.co/wordpress/24978/cyber-crime/al-qaeda-encryption-tools.html

74 http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085

75 http://www.thedailybeast.com/articles/2015/03/23/isis-hackers-googled-their-hit-list-troops-names-were-already-on-public-websites.html
http://www.dataleakes.net/feds-charge-ardit-ferizi-aka-th3dir3ctory-with-creating-hit-list-of-american-military-govt-employees-for-isis/

76 Este es el caso por ejemplo de la revelación de información arsenal de soldados y empleados norteamericanos (véase: http://www.dataleakes.net/jihadist-leaks-addresses-of-army-sgt-dillard-johnson-navy-seal-rob-oneill/), así como listas de empleados europeos (véanse: http://www.ubergizmo.com/2015/12/islamic-cyber-army-responds-to-isis-day-of-trolling/ y
https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/site-6-1-15-ishd-calls-for-attacks-on-10-italian-army-personnel.html). La publicación de estos datos perseguía animar a sus seguidores a perpetrar acciones contra tales objetivos personales.

77 Véanse: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&tagId=787&Itemid=1355
http://www.washingtontimes.com/news/2016/mar/15/islamic-state-hackers-post-kill-list-minnesota-cop/

78 Véanse: http://www.techworm.net/2015/09/isis-affiliates-to-launch-cyber-attacks-on-united-states-to-celebrate-911.html
http://abcnews.go.com/US/fbi-warns-isis-inspired-cyber-attacks-911-anniversary/story?id=33684413

79 Por ejemplo, en junio de 2016, distintos medios informaron que ciertos ataques desarrollados en nombre del Cyber Caliphate e ISIS fueron efectivamente desarrollados por elementos aliados con Rusia. (véase: http://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand/).

80 Las protestas on-line, las huelgas, el ciber-activismo, las campañas de peticiones y el boicot on-line están aumentando. Por ejemplo, la red de activismo y peticiones on-line Avaaz.org creció alrededor de 40 millones de miembros en ocho años, y Change.org tiene en la actualidad 80 millones de usuarios.

se han concentrado en el desarrollo de ataques DDoS a objetivos gubernamentales[81], medios de comunicación[82] y organizaciones privadas[83]. En otros casos, las acciones también se han dirigido a desvelar determinados comportamientos[84] o datos personales de instituciones gubernamentales[85].

Como hemos señalado, las capacidades mostradas por los grupos en sus ataques son muy variadas, llegando a alcanzar un alto grado de sofisticación[86] [87].

Es frecuente observar que las acciones se incrementan durante conflictos nacionales o internacionales. Así sucedió tras los ataques yihadistas en París y Bruselas, en los que se incrementaron las desfiguraciones de páginas web y los ataques DDoS por parte de grupos, en nombre de Anonymous, en algunos casos- en contra y a favor de simpatizantes de Daesh[88].

El ciberactivismo de raíz española en 2016 ha sido prácticamente inexistente en términos operacionales de ciberataque salvando la actividad ofensiva desplegada por 'La 9ª Compañía', que ha comprometido algunos sitios web de algún Ayuntamiento, un par de medios de comunicación, algunas empresas y cámaras de comercio.

Además de 'La 9ª Compañía' y al margen de alguna acción ocasional de identidades aisladas, el colectivo 'Anonymous' autóctono puede considerarse tanto inactivo operativamente como carente de impacto en términos de propaganda en España. Véase, para mayor información, "Informe de Amenazas CCN-CERT IA-04/17 - Hacktivismo y Ciberyihadismo - Informe Resumen 2016."

En Iberoamérica 2016 ha mostrado un debilitamiento general de las entidades en la órbita de 'Anonymous', dejando preeminencia a identidad con marca propia. Estas identidades, no obstante, decayeron en sus acciones hacia finales de año. El debilitamiento de 'Anonymous' se ha traducido en un menor número y recorrido de marcos narrativos planteados en los países de la región en 2016, muchos de los cuales han resultado en una baja volumetría de ciberataques y en bajo impacto.

A nivel internacional en 2016 ha puesto de manifiesto que, aunque se producen varios miles de ciberataques al día con este origen en todo el mundo ejecutados por varias decenas de identidades, no hay más de media decena de ellas que pueden considerarse una ciberamenaza de nivel medio, capaces no sólo de explotar las

81http://spd.rss.ac/aHR0cDovL25ld3Muc29mdHBlZGlhLmNvbS9uZXdzL2Fub255bW91cy1oYWNrcy11cy1kZXBhcnRtZW50LW9mLWFncmljdWx0dXJlLXRvLXByb3Rlc3QtYWdhaW5zdC1tb25zYW50by00OTU4NTUuc2h0bWw

82 Véanse: http://www.rcfp.org/browse-media-law-resources/news/online-attacks-against-media-websites-are-increasing-and-costly

https://www.hackread.com/anonymous-ddos-zimbabwe-herald-website/

83 Véanse: http://www.scmagazineuk.com/anonymous-attacks-two-japanese-airports/article/447817/

http://www.bbc.com/news/technology-35306206

84 Tal es el caso, por ejemplo, de la revelación realizada por un grupo hacktivista respecto de cuentas de miembros del Ku Klux Klan (véase: http://www.ibtimes.co.uk/anonymous-hackers-threaten-reveal-identities-1000-ku-klux-klan-members-opkkk-1525758)

85 Como sucedió con la revelación de nombres y credenciales de miembros de ciertas organizaciones de la defensa de Israel (véase: https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/anonsec-allegedly-hacks-israel-missile-defense-association.html,).

86 Véanse: http://tweakers.net/nieuws/109245/hackers-stelen-gegevens-van-anti-ddos-dienstverlener-staminus.html

https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

87 Quizás lo más significativo fue el incidente de febrero de 2016, en el que se anunció que un grupo de personas habían atacado un dron de la NASA con la intención de estrellarlo en el mar.

88 Véanse: http://www.eteknix.com/major-isis-messaging-forum-taken-anonymous/

http://www.zdnet.com/article/isis-supporter-cyber-caliphate-takes-over-54000-twitter-accounts/#ftag=RSSbaffb68

vulnerabilidades más comunes para comprometer sitios web sino de aplicar varios tipos de técnicas para lograr acceso a sus servidores y contenidos en objetivos.

Como novedad respecto de años previos, en 2016 se han detectado un par de casos de identidades mostrando rasgos de Indonesia que han insertado mecanismos de distribución de malware (adware) en servidores web atacados por desfiguración. Adicionalmente, una identidad hacktivista en Brasil profirió amenazas, no cumplidas, de realizar un ciberataque mediante ransomware. Esta intersección entre ciberactivismo y cibercriminales convencionales (distribución de malware) se considera de momento ocasional y no representa un patrón en el modus operandi hacktivista.

5.5 Cibervándalos y script kiddies

Durante 2016 se ha observado un importante crecimiento de las acciones de estos agentes, motivadas en buena parte por el incremento de herramientas accesibles para la perpetración de ataques. Estos actores desarrollan sus acciones como un reto, para demostrar sus propias capacidades o como una simple broma, lo que induce a pensar que, en ocasiones, puede tratarse de menores.

Sobre el uso de herramientas accesibles, en 2016 se ha evidenciado el uso de los llamados Booter-Services (DDoS-As-A-Service) como mecanismos para la perpetración de ataques DDoS, lo que posibilita que una acción de este tipo pueda ser desarrollada con escasos recursos económicos y limitados conocimientos[89].

En el plano internacional, algún ejemplo de ataque dirigido realizado por este tipo de actores fue el desarrollado por el grupo denominado "Crackas with attitude", dirigido contra directivos de ciertas unidades de inteligencia norteamericanos[90], que derivó en la publicación en internet de datos de empleados de la CIA y del FBI.

Las plataformas de juegos on-line también han constituido objetivos muy populares para este tipo de ataques[91]. Sea como fuere, la atribución de este tipo de ataques es extraordinariamente difícil[92], todo ello sin olvidar que, en ocasiones, el mismo ataque es reivindicado desde diferentes partes[93].

5.6 Actores internos y ciberinvestigadores

Las amenazas derivadas de acciones de actores internos suelen corresponderse con empleados o exempleados descontentos que, por razones económicas, políticas o personales, manipulan deliberadamente los sistemas para apoderarse de información[94]

89 Algunos ejemplos de esto han sido los ataques DDoS contra Ziggo y Volksrant.

90 En concreto, contra John Brenan (véase: https://www.theguardian.com/technology/2015/oct/19/cia-director-john-brennan-email-hack-high-school-students) y James Clapper (véase: http://www.theguardian.com/us-news/2016/jan/13/hacker-breaks-into-personal-email-of-us-director-of-national-intelligence). El autor fue un menor de dieciséis años.

91 Véanse: http://news.softpedia.com/news/phantom-squad-starts-christmas-ddos-attacks-by-taking-down-ea-servers-498078.shtml

http://www.csmonitor.com/World/Passcode/2015/1224/Lizard-Squad-plans-Christmas-Day-encore-with-Xbox-PlayStation-attacks

http://www.engadget.com/2015/12/30/steams-christmas-privacy-issues-affected-34-000-users/

92 Un ejemplo lo encontramos en el importante ataque sufrido por la BBC, cuya autoría se atribuía un autor relacionado con actividades anti yihadistas (véase: http://www.bignewsnetwork.com/news/239915393/anti-isis-hackers-say-they-took-down-bbc-website-during-testing).

93 http://www.techworm.net/2015/12/hacking-group-skidnp-takes-down-phantom-squads-website.html

94 http://www.newsobserver.com/news/business/article32944404.html

sensible, aunque no suelen representar riesgos importantes en la mayor parte de los casos.

Por su parte, los ciberinvestigadores son individuos que persiguen el descubrimiento de vulnerabilidades en los sistemas de información al objeto de mostrar públicamente un inadecuado nivel de seguridad. Esta publicidad hace que, en muchas ocasiones, los sistemas descritos sean temporalmente vulnerables.

En los últimos años ha tomado carta de naturaleza la práctica de la denominada **Revelación Responsable** (*Responsible Disclosure*) como un mecanismo para satisfacer los intereses de los ciberinvestigadores sin poner en peligro la seguridad de las organizaciones. Al hilo de esta cuestión, se ha extendido la tendencia de establecer un mecanismo de Recompensa por vulnerabilidades (Bugs), en el que los investigadores se comprometen a no revelar estas a cambio de" recompensas"[95].

5.7 Organizaciones privadas

Aunque las amenazas provenientes de las organizaciones privadas pueden tener como objetivo dejar fuera de juego los sistemas de información de las organizaciones rivales, 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.

En 2016 se han observado algunos casos de este tipo de acciones96.

El cuadro siguiente muestra un resumen de los actores estudiados y sus motivaciones habituales.

Actores	Motivaciones
Estados	Mejorar su posición geopolítica o estratégica.
Ciberdelincuentes	Beneficio económico (directo o indirecto).
Ciberterroristas	Alterar el normal desenvolvimiento social, atemorizar a la población o influir en las decisiones políticas.
Ciberyihadistas	Propaganda, reclutamiento.
Ciberactivismo	Ideología.
Cibervándalos y script kiddies	Evidenciar vulnerabilidades, piratería, diversión, retos.

95 Tal es el caso del Pentágono norteamericano (véase: http://www.wired.co.uk/news/archive/2016-03/02/hack-the-pentagon-bug-bounty) y la empresa General Motors (véase: https://hackerone.com/gm).

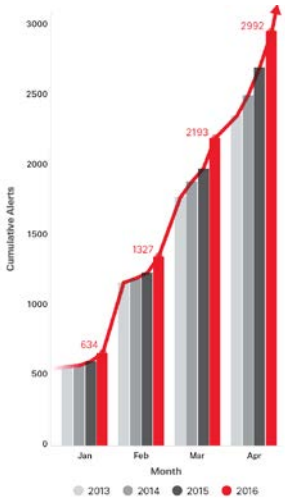
96 Un par de ejemplos: en los Estados Unidos se produjo un ataque de los empleados de una empresa proveedora de productos textiles a otra empresa de la competencia (véase: https://www.security.nl/posting/453200/IT-directeur+Amerikaans+bedrijf+hackte+server+concurrent). También en Estados Unidos, un ataque entre competidores de baseball (véase: https://nakedsecurity.sophos.com/2016/01/12/ex-cardinals-exec-yes-i-hacked-rival-astros-database/). Revelaciones a terceros competidores de los datos obtenidos en el ataque a Ashley Madison (véase: http://krebsonsecurity.com/2015/08/leaked-ashleymadison-emails-suggest-execs-hacked-competitors/).

Ciberinvestigadores	Evidenciar debilidades, autoafirmación.
Actores internos	Venganza, beneficio económico, motivos ideológicos.
Organizaciones privadas	Ciberespionaje: obtención de información de valor.

6. VULNERABILIDADES

Como es sabido, una vulnerabilidad es una propiedad de las TIC, de las organizaciones o de los usuarios que permite que uno o varios agentes de las amenazas desarrollen ataques sobre los sistemas de información de sus víctimas.

El número de vulnerabilidades sigue en permanente crecimiento. La figura siguiente muestra la evolución en el número acumulado de alertas, en el primer cuatrimestre de 2016[97].



Los siguientes epígrafes revisan las vulnerabilidades más significativas evidenciadas durante 2016.

6.1 El software: su industria, desarrollo y aplicación

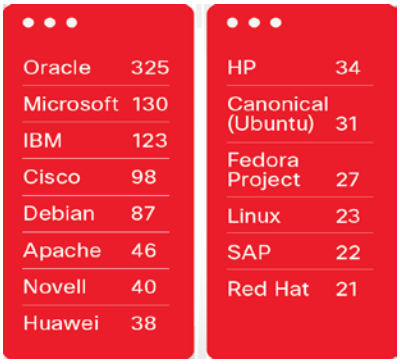
Destacan las siguientes:

El software como cadena de montaje: Como se ha dicho, 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 tales componentes presenta una vulnerabilidad el resultado final será asimismo vulnerable[98].

97 Fuente: CISCO: 2016 Midyear Cybersecurity Report.

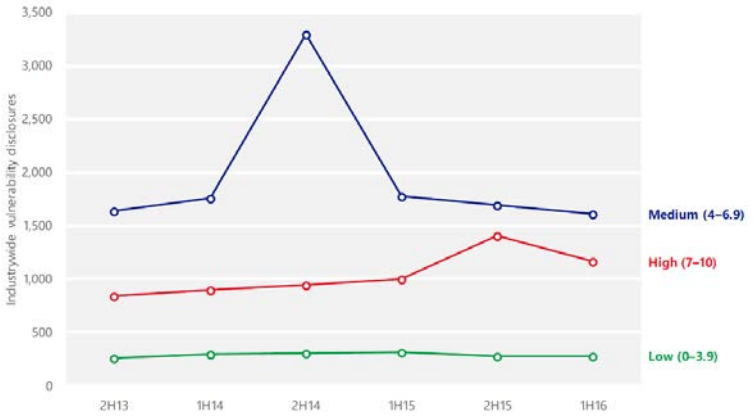
98 Unos ejemplos: en agosto de 2015 se descubrieron determinadas vulnerabilidades en software preinstalado en productos Lenovo (véase: http://www.theregister.co.uk/2015/08/12/lenovo_firmware_nasty/). Por su parte, la compañía de Taiwán D-Link, filtró de manera accidental una de sus claves de firma de software, lo que provocó que ciertos agentes de las amenazas utilizarán firmas legítimas de D-Link para desplegar código dañino (véase: http://www.theregister.co.uk/2015/09/18/d_link_code_signing_key_leak/). Otro más: El firmware de ciertos routers de la empresa Cisco estaba equipado con una puerta trasera que posibilitaba su manipulación (véase: https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html).

La figura siguiente muestra el número de vulnerabilidades detectadas, por fabricante, en el periodo comprendido entre el 1 de Enero y el 30 de Marzo de 2016[99].



Haciendo una proyección temporal más amplia -hasta octubre de 2016-, la figura siguiente muestra exclusivamente las vulnerabilidades críticas notificadas en el software habitual[100].

Por su parte, la figura siguiente muestra la evolución en el tiempo del número de vulnerabilidades descubiertas, atendiendo a su gravedad[101] [102].



La seguridad en la formación de desarrolladores: Gran parte de los programas formativos generales dirigidos a alumnos de programación prestan poca o nula atención a la seguridad, quedando esta disciplina, la mayor parte de las veces, reservada a los

99 Fuente: Cisco Security Research.

100 Fuente original: National Vulnerability Database (NVD), procesado por Cisco ("2017 Annual Cybersecurity Report".)

101 El Common Vulnerability Scoring System (CVSS) es un sistema de puntuación normalizado e independiente de la plataforma, utilizado para calificar las vulnerabilidades IT. La métrica base CVSS asigna un valor numérico entre 0 y 10 a vulnerabilidades basadas en factores tales como impacto potencial, vectores de acceso y facilidad de explotación. Las puntuaciones más altas representan mayor gravedad.

102 Fuente: Microsoft Security Intelligence Report Volume 21 | January through June, 2016.

estudios universitarios o programas especializados. La industria del software no es ajena a esta realidad, que hace primar la funcionalidad de un software y su velocidad frente a un comportamiento seguro.

La interconexión de Sistemas de Control Industrial: La inseguridad del software se vuelve especialmente delicada cuando se trata de software para Sistemas de Control Industrial, muy especialmente cuando tales sistemas se encuentran interconectados a través de internet. Un software inseguro, instalado en un sistema determinado, genera inseguridad en todos aquellos a los que se conecta[103].

La actualización del software: La experiencia nos ha demostrado que muchas de las brechas de seguridad son debidas a la existencia de vulnerabilidades que llevaban tiempo siendo conocidas por la comunidad[104]. Aunque los riesgos han sido puestos de manifiesto en repetidas ocasiones, todavía puede encontrarse en muchas organizaciones -públicas y privadas- equipamiento o informático que no se encuentra debidamente actualizado con las últimas actualizaciones, afectando no sólo a los PC de usuario sino también -lo que es peor- a servidores corporativos[105]. Todo ello sin entrar a considerar el importante parque informático existente en la actualidad sustentado en software o sistemas operativos para los que no existen actualizaciones. Esta realidad se extiende igualmente a una multiplicidad de dispositivos móviles, relativamente recientes en el tiempo, pero cuyos fabricantes han dejado de actualizar.

La eficacia de las medidas anti-amenazas: Aunque, en general, las grandes organizaciones disponen de medidas de seguridad de la información que comprenden la utilización de una multiplicidad de recursos, son todavía muchas las empresas e instituciones públicas cuya única medida de seguridad es el software antivirus, muchas veces desactualizado. Estas organizaciones inseguras, cuando están conectadas con otras, desplazan hacía estas últimas su propia inseguridad. En un mundo interconectado los defectos de seguridad de un elemento pueden repercutir gravemente en la seguridad de los que se encuentran interconectados con él. Una organización mal protegida es una víctima fácil para todo tipo de actores (estados o ciberdelincuentes) que, en muchas ocasiones, no tendrán que utilizar mecanismos sofisticados para penetrar en las redes de sus víctimas.

La publicidad de las vulnerabilidades: 2016 ha seguido mostrando la tendencia de los últimos años en lo que respecta a la publicidad de campañas relativas a vulnerabilidades de naturaleza técnica[106]. El peligro, en este caso, proviene de dos fuentes: la exhibición pública de determinadas vulnerabilidades puntuales (que ponen en grave riesgo a los sistemas afectados) y una exagerada publicidad de determinado tipo

103 Y todo ello, pese a la existencia de diferentes productos y servicios para Pruebas de Seguridad de Aplicaciones (AST, por sus siglas en inglés), diseñados para analizar y verificar aplicaciones en busca de vulnerabilidades de seguridad, usando tecnologías AST estáticas (SAST), dinámicas (DAST) e interactivas (IAST). (Véase: Gartner: "Magic Quadrant for Application Security Testing", para obtener una lista exhaustiva de tales herramientas).

104 Fuente: Verizon 2016 Data Breach Investigations Report (véase: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf).

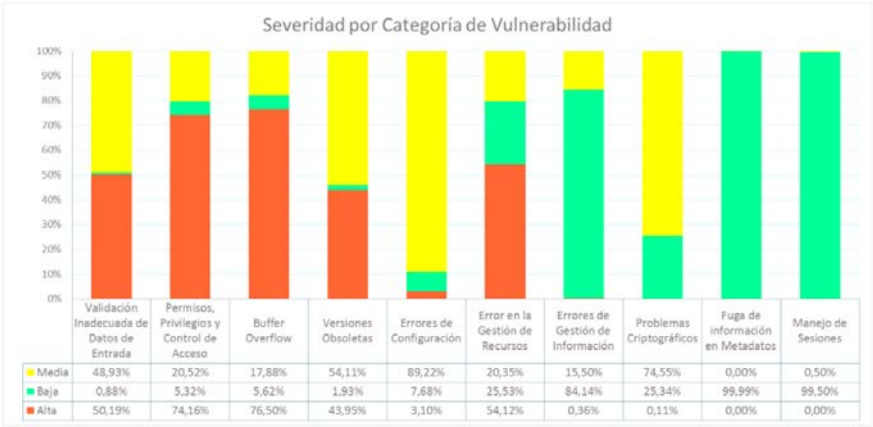
105 Véanse: Microsoft Windows Update for Business (https://blogs.windows.com/windowsexperience/2015/05/04/announcing-windows-update-for-business/) http://www.itwire.com/business-it-news/open-source/67655-linux-40-released-includes-live-patching

106 Cyber Security Assessment Netherlands 2015 (https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-5/1/CSBN5.pdf).

de vulnerabilidades, que, inadvertidamente, hacen pasar desapercibidas otras más críticas.

Telefónica ha hecho público el siguiente gráfico-resumen de distintos tipos de vulnerabilidades, entre las que se incluyen, atendiendo a datos obtenidos durante el primer semestre de 2016[107].

Del mismo informe, se incluye el gráfico siguiente, que muestra la severidad de las antedichas vulnerabilidades, atendiendo al criterio establecido por CVSS v2[108].



En el portal del CCN-CERT[109], en 2016, se publicaron un total de 3.773 parches (2.460 en el primer semestre, y 1.313 en el segundo semestre) publicados por los siguientes fabricantes:

107 Fuente: Telefónica: Tendencias en Vulnerabilidades. 1S - 2016.

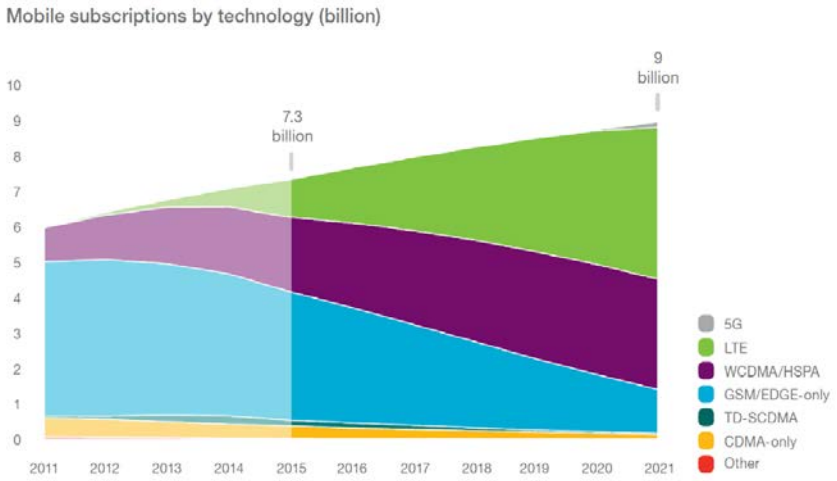
108 https://www.first.org/cvss/v2/guide

109 https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades.html

Fabricante	Parches 1er semestre	Parches 2do semestre	Acumulado 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**
Totales	**2.460**	**1.313**	**3.773**

6.2 Hallazgos en el lado del usuario

La comercialización de dispositivos móviles sigue un ritmo acelerado. La figura siguiente muestra la distribución actual y previsible de equipamiento móvil, atendiendo a la tecnología usada[110].

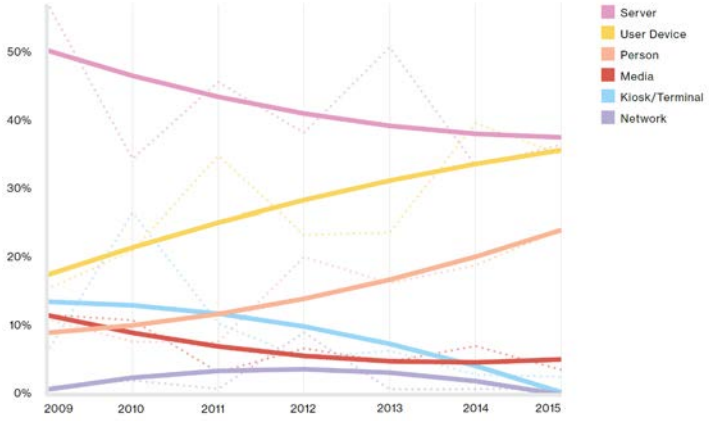


Los fabricantes, motivados por el interés de mantenerse a la cabeza, vienen siendo capaces de comercializar varios productos al año, cada uno de los cuales puede llegar a ejecutar un sistema operativo distinto del anterior. Como quiera que la vida útil de tales dispositivos es muy limitada (2 años es lo habitual), muchos fabricantes, transcurrido ese tiempo dejan de publicar actualizaciones para tales productos, lo que los convierte en víctimas para los ciberataques.

La figura siguiente muestra el porcentaje de brechas de seguridad por categoría de activo[111].

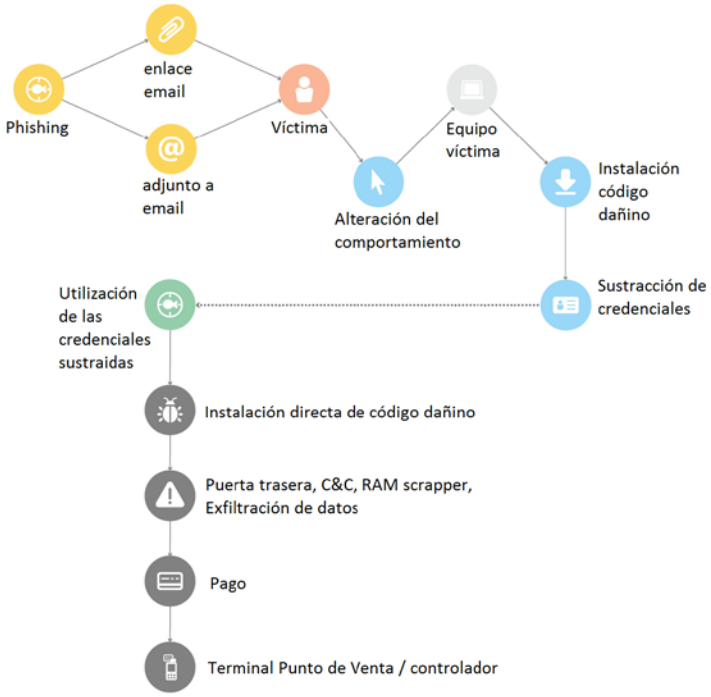
110 Fuente: Ericsson: Mobility Report. (Junio, 2016).

111 Fuente: Verizon: 2016 Data Breach Investigations Report.

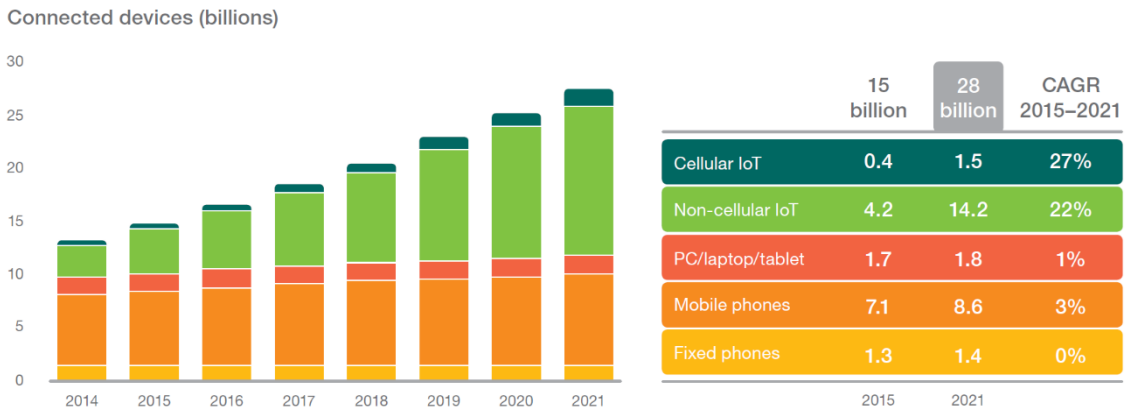


Por lo que respecta a la sensibilización sobre la ingeniería social, los atacantes continúan redoblando sus esfuerzos para persuadir a sus víctimas a que realicen determinadas acciones. Así, durante 2016 hemos visto como muchos usuarios -personales o corporativos- han caído en la trampa del phishing a través de correo electrónico, o, incluso, de llamadas telefónicas (cuyo incremento en 2016 ha sido espectacular). Como se ha demostrado cuando la ingeniería social se dirige específicamente a sectores individualizados, a organizaciones o a personas concretas, el porcentaje de éxito o de los atacantes crece exponencialmente. Aunque, en muchas ocasiones, no es fácil distinguir un mensaje real de otro fingido, se ha demostrado que las campañas de sensibilización para usuarios finales son más efectivas cuando animan a tales usuarios a alterar su comportamiento ante una determinada situación.

La figura siguiente muestra el itinerario dañino más frecuente seguido por los agentes de las amenazas.



Por su parte, el peligro del internet de las cosas, con el crecimiento de los dispositivos conectados a Internet, sigue en aumento. La figura siguiente muestra unas estimaciones al respecto (1 billón= Mil millones)[112].



	15 billion	28 billion	CAGR 2015–2021
Cellular IoT	0.4	1.5	27%
Non-cellular IoT	4.2	14.2	22%
PC/laptop/tablet	1.7	1.8	1%
Mobile phones	7.1	8.6	3%
Fixed phones	1.3	1.4	0%
	2015	2021	

No es necesario insistir en la multiplicidad de aplicaciones y dispositivos que se conectan a internet, incluso en el terreno doméstico. Desafortunadamente, muchos de sus fabricantes no parecen ser conscientes de los riesgos que supone tal conexión, lo que provoca que muchos de tales equipamientos se estén utilizando conteniendo graves vulnerabilidades de software[113], lo que, en ocasiones, impacta directamente en la seguridad pública.

Desarrollos técnicos

Las **vulnerabilidades de TLS**: El Transport Layer security (TLS) es un protocolo mundialmente utilizado a la hora de construir conexiones a internet seguras. Esta realidad provoca dos reacciones de sentido opuesto: el interés de los ciberinvestigadores por descubrir nuevas vulnerabilidades en TSL y la aparición de nuevos métodos de ataque dirigidos a aplicaciones TSL[114].

Adobe Flash Player: en 2015 se solucionaron más de 330 vulnerabilidades de este software, incluyendo 8 vulnerabilidades de día cero[115]. Que Flash Player continúe durante 2016 ocupando las primeras posiciones en software vulnerable no parece ser una novedad[116], aunque es cierto que su uso está mostrando un claro declive[117]. La propia compañía Adobe no parece muy interesada en mantener Flash durante mucho más tiempo[118]. No obstante, buena parte de los juegos on-line, así como software legacy, entre otros, siguen usando Flash.

112 Fuente: Ericsson: Mobility Report. (Junio, 2016).

113 Durante los últimos años ha cobrado especial relevancia las vulnerabilidades del software instalado en automóviles. Así, en el verano de 2015, ciertos modelos de automóviles fabricados por Ford, Range Rover, Toyota, Chrysler, Tesla y Chevrolet, presentaban vulnerabilidades, algunas de las cuales no podían ser corregidas automáticamente. Véanse: F-Secure Threat Report 2015 (https://www.f-secure.com/documents/996508/1030743/Threat_Report_2015.pdf) http://www.wired.com/2015/09/chrysler-gets-flak-patching-hack-via-mailed-usb/

114 En particular, la vulnerabilidad Drown obtuvo un amplio eco en marzo de 2016.

115 Common Vulnerabilities and Exposures (https://cve.mitre.org/).

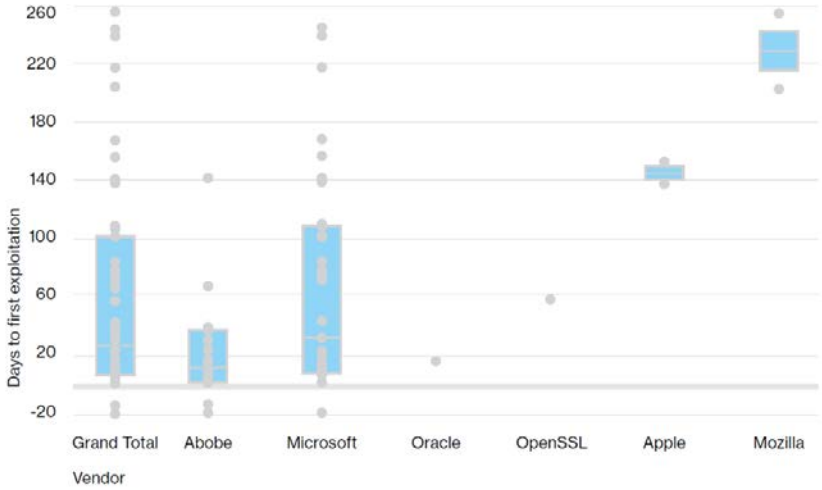
116 NTT Group Global Threat Intelligence Report (https://www.solutionary.com/_assets/pdf/research/2016-gtir.pdf).

117 Muchas de las páginas web más populares (tales como Facebook y Youtube) han cambiado a HTML5 para ejecutar vídeos.

118 300 Welcome Adobe Animate CC (http://blogs.adobe.com/animate/welcome-adobe-animate-cc-a-new-era-for-flash-professional/).

La figura siguiente muestra la incidencia de las vulnerabilidades usadas por exploits-kits dirigidos a Flash[119], en el primer cuatrimestre de 2016.

La figura siguiente representa el tiempo transcurrido entre la publicación y la primera explotación con éxito observada por los fabricantes120. Puede apreciarse que las vulnerabilidades de Adobe se explotan rápidamente, mientras que las vulnerabilidades de Mozilla tardan mucho más en explotarse tras la divulgación. La mitad de todas las explotaciones ocurren entre 10 y 100 días después de la publicación de la vulnerabilidad, con una media de 30 días[121].



La **ocultación del código dañino**: detectar código dañino se torna una tarea más difícil cuando tal código no se ejecuta en la memoria del dispositivo y sí en el firmware de componentes periféricos de un ordenador. Durante 2016, este tipo de técnicas han sido extraordinariamente reforzadas por los atacantes[122]. Lo especialmente peligroso de este

119 Fuente: Cisco Security Research.

120 Las casillas azules representan el 50% de los valores para una categoría dada y la línea gris dentro de la casilla es el valor medio. Los puntos representan valores individuales.

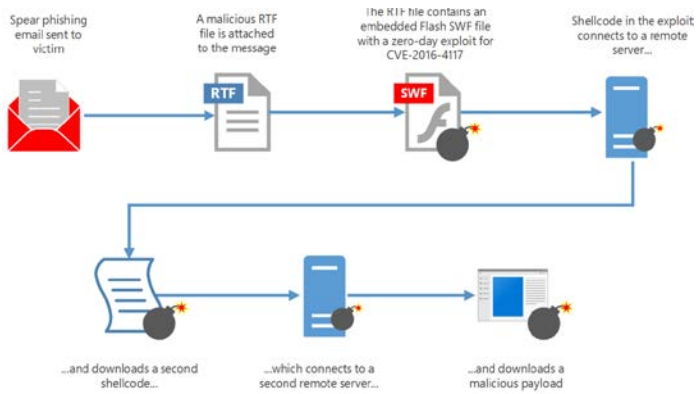
121 Fuente: Verizon: "2016 Data Breach Investigations Report".

122 Unos ejemplos: se han evidenciado casos de instalación de código dañino en la tarjeta de video de un ordenador (véase: http://www.securityweek.com/gpu-malware-not-difficult-detect-intel-security) o en el firmware de un módem LTE (véase: http://www.fiercecio.com/story/security-researchers-hide-malware-firmware-lte-modem/2015-08-10), o en una tarjeta SSD (véase: https://www.computable.nl/artikel/nieuws/security/5408780/250449/hackinggroep-herprogrammeert-ssd-firmware.html) o en un disco duro (véase: http://arstechnica.com/information-technology/2015/02/how-hackers-could-attack-hard-drives-to-create-a-pervasive-backdoor/) o en el firmware de un router (véase: http://news.softpedia.com/news/cisco-routers-infected-with-boot-resistant-malware-491835.shtml).

tipo de ataques es que posibilita el mantenimiento de la infección incluso después de haber reinstalado el sistema operativo. En muchas ocasiones, desafortunadamente, las medidas de seguridad no son capaces de detectar el código dañino oculto.

Ataques por exploits día-cero: los ataques PROMETHIUM y NEODYMIUM dirigidos a individuos de una zona específica de Europa[123], fueron ejemplo de ello. Aunque la mayor parte del actual código dañino persigue beneficios económicos directos, en 2016 ambos grupos de actividad parecieron buscar información concreta sobre individuos específicos. En mayo de 2016, ambos se utilizaron para lanzar ciberataques, aunque con una infraestructura completamente distinta, lo que indicaba una falta de asociación a nivel operativo. Sin embargo, la similitud en la localización de las víctimas de las campañas, la sincronización y el uso del mismo exploit día-cero conduce a pensar que ambos grupos pudieran estar relacionados, quizás a un nivel superior.

La figura siguiente muestra la cadena de ataque de NEODYMIUM y cómo se explotó la vulnerabilidad CVE-2016-4117 para infectar los ordenadores de las víctimas[124].



7. MÉTODOS DE ATAQUE

Con cada edición del presente informe, observamos que los agentes de las amenazas continúan mejorando sus métodos de ataque y las herramientas que utilizan para perpetrarlos. Los siguientes epígrafes describen los métodos de ataque más usados durante 2016.

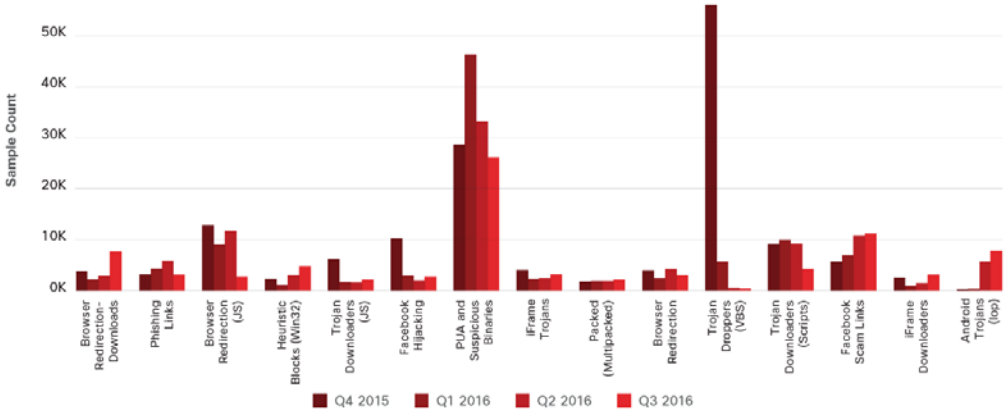
7.1 Código dañino

La figura siguiente muestra la presencia del código dañino más habitual, desde finales de 2015 hasta el tercer semestre de 2016[125].

123 Básicamente: Turquía, Estados Unidos, Alemania y Reino Unido.

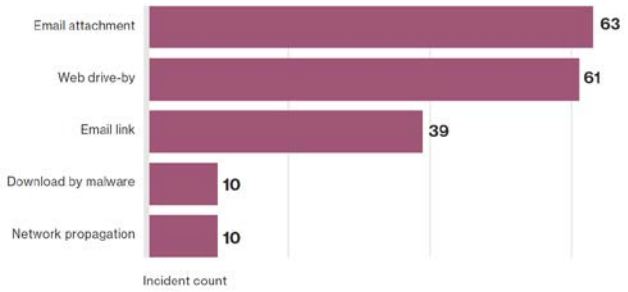
124 Fuente: Microsoft Security Intelligence Report Volume 21 | January through June, 2016.

125 Fuente: Cisco security Research. "2017 Annual Cibersecurity Report".



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 por el CERT Gubernamental Nacional en el sector público y en empresas de interés estratégico, el 53,6% (11.237) correspondían con la tipología de código dañino y, dentro de esta, los troyanos (con el 86,64% de los casos) y el ransomware (9,2%) fueron los de mayor incidencia

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



El **Ransomware** constituye la variante de código dañino que más ha afectado a los sistemas de información de todo el mundo durante 2016. Como se ha dicho, su peligrosidad deriva tanto de una mayor direccionalidad de los ataques como de una mejora sustancial en su base tecnológica.

Aunque la mayor parte de estos ataques culminan con el éxito, se ha podido observar que, en ciertos casos, un error de implementación del código dañino ha permitido a las víctimas descifrar los ficheros atacados.

Por otro lado, durante 2016, ciertas variantes de Ransomware han empezado a afectar a plataformas de usuario que no habían sido atacadas durante los años anteriores. Tal ha sido el caso, por ejemplo, del código dañino *KeRanger*, que ha atacado a sistemas Mac OS X[126]. Por otro lado, la creciente conectividad de equipos de todo tipo ha venido a multiplicar el efecto del ransomware[127].

Además de los equipos de usuario, el Ransomware también ha afectado a servidores[128], con lo que, además de en obtener los beneficios derivados del rescate de los ficheros, los atacantes se han servido de este mecanismo para introducirse en las redes de sus víctimas, expandiendo la cobertura del Ransomware a una multiplicidad de equipos.

Al objeto de hacer más fuerza en las víctimas, además de solicitar el rescate para descifrar los ficheros, los atacantes han empezado a amenazar a las víctimas con divulgar los datos personales a los que han accedido si no se satisface la cuantía de la extorsión[129].

Otro método de ataque observado en 2016 ha sido el de **infectar sitios tradicionalmente confiables**, como las tiendas oficiales de aplicaciones para dispositivos móviles. Un buen ejemplo de este mecanismo lo constituyen los ataques por Watering Hole. Así, una vez comprometido el website de un proveedor de aplicaciones, el código dañino se incrusta en determinadas aplicaciones descargadas por los usuarios -habiendo sido, incluso, firmado electrónicamente[130]- facilitando la diseminación de la infección[131]. Otro procedimiento ha sido la infección de entornos de desarrollo (Integrated development environments, IDE)[132].

126 Véanse: http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/
https://blog.malwarebytes.org/exploits-2/2013/07/qa-about-the-latest-html-ransomware-affecting-mac-os-x-users/

127 Durante 2016, la compañía Symantec ha llevado a cabo un estudio en relación con el Ransomware en dispositivos Android, en el que ha podido apreciar se la infección de smart-watchs a través de smart-phones (véanse: http://www.welivesecurity.com/wp-content/uploads/2016/02/Rise_of_Android_Ransomware.pdf y http://www.symantec.com/connect/blogs/dawn-ransomwear-how-ransomware-could-move-wearable-devices).

128 Véanse: http://www.cio.com/article/3052553/server-software-poses-soft-target-for-ransomware.html#tk.rss_security
https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html

129 https://www.secureworldexpo.com/new-ransomware-threatens-publish-personal-information

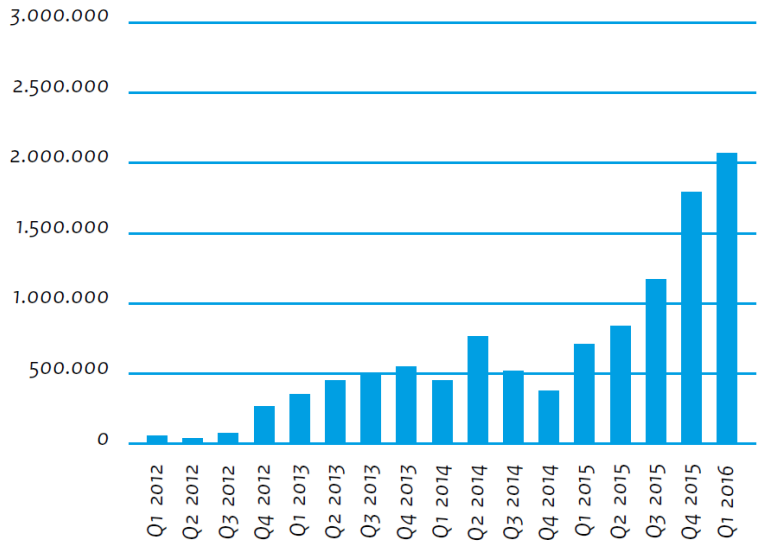
130 http://www.computerworld.com/article/3044728/security/cyberespionage-groups-are-stealing-digital-certificates-to-sign-malware.html

131 Durante 2016 hemos presenciado ataques de este tipo a los websites de Linux Mint (véase: http://blog.linuxmint.com/?p=2994,) y Transmission (véase: http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/).

132 Este método ha sido el usado en China para difundir código dañino a través de copias de Apple Xcode IDE, de forma que todas las aplicaciones desarrolladas con este entorno contenían código dañino, lo que podría concluir con la infección de aplicaciones accesibles a través de la tienda oficial Apple (véase: https://blog.malwarebytes.org/mac/2015/09/xcodeghost-malware-infiltrates-app-store/ y http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/ y http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/).

La presencia de atacantes infiltrados en los **equipos de desarrollo** oficiales, permite el desarrollo de nuevos productos software en los que se incluye, "de fábrica", código dañino[133]. Esta problemática puede darse tanto en los propios fabricantes de software como en los revendedores[134].

La masiva utilización de **dispositivos móviles** (smartphones y tablets, especialmente) en todo tipo de aplicaciones, particulares o de negocio, ha convertido a este equipamiento o en uno de los preferidos para albergar código dañino. La figura siguiente muestra el crecimiento de instancias de este tipo de código dañino para Android desde 2012 al primer trimestre de 2016[135].



Según las observaciones hechas, la infección de dispositivos móviles tiene lugar, principalmente, a través de aplicaciones descargadas de tiendas no oficiales o infecciones provocadas por la "liberación" de dispositivos de infecciones generadas a partir de entornos de desarrollo infectados.

Aunque Android sigue constituyendo el objetivo principal de los agentes de las amenazas, los ataques dirigidos a iOS siguen en aumento[136], especialmente cuando el ataque se deriva de una aplicación que ha podido ser generada a partir de una herramienta de desarrollo o previamente infectada[137]. Durante 2016 se han observado casos de código dañino que explotan ciertas vulnerabilidades en iOS, lo que les permite

133 Véanse:
https://www.sophos.com/en-us/press-office/press-releases/2006/10/ipod-ships-with-virus.aspx https://www.sophos.com/fr-fr/press-office/press-releases/2007/01/tomtom.aspx

134 El uso de este mecanismo de infección ha sido especialmente visible durante 2016 en teléfonos y tablets Android provenientes de China (véase: https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q2_2015_US.pdf y http://www.ibtimes.co.uk/amazon-selling-least-30-brands-cheap-chinese-android-tablets-infected-cloudsota-malware-1528442).

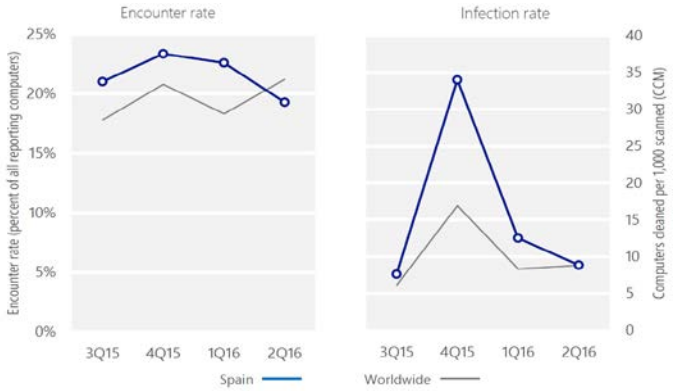
135 Fuente: AV-Test.

136 Véanse: https://www.theiphonewiki.com/wiki/Malware_for_iOS https://blog.fortinet.com/post/ios-malware-does-exist

137 https://www.fireeye.com/blog/threat-research/2015/11/ibackdoor_high-risk.html

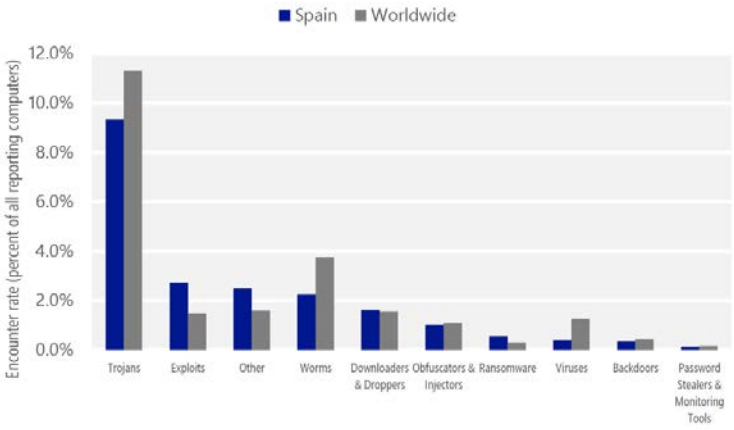
instalarse en los equipos de las víctimas sin necesidad de ninguna autorización por parte del usuario[138].

La figura siguiente muestra la evolución en España de la tasa de localización (*encounter rate*) de código dañino y la tasa de infección (*infection rate*) en la última mitad de 2105 y la primera de 2016[139].



Como puede observarse, en el segundo trimestre de 2016, el 19,3% de los ordenadores se enfrentaron a código dañino, algo menor que la tasa mundial (20,8%). Por otro lado, se detectó y eliminó el código dañino en el 8,9 por mil de los ordenadores infectados.

Respecto de los tipos de código dañino y siguiendo con la misma fuente, la categoría de este tipo de software más común en España fueron los Troyanos (encontrándose en el 9,3% de los ordenadores sujetos a análisis), seguidos por los Exploits (2,7%).



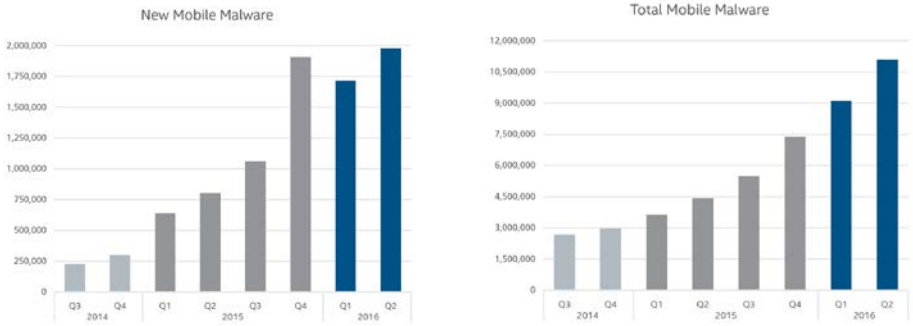
La tabla siguiente muestra las instancias de código dañino más encontradas en España, utilizando la herramienta de análisis en tiempo real de Microsoft, sobre ordenadores con sistema operativo de este fabricante.

138 Tal ha sido el caso, por ejemplo, del código dañino AceDeceiver.

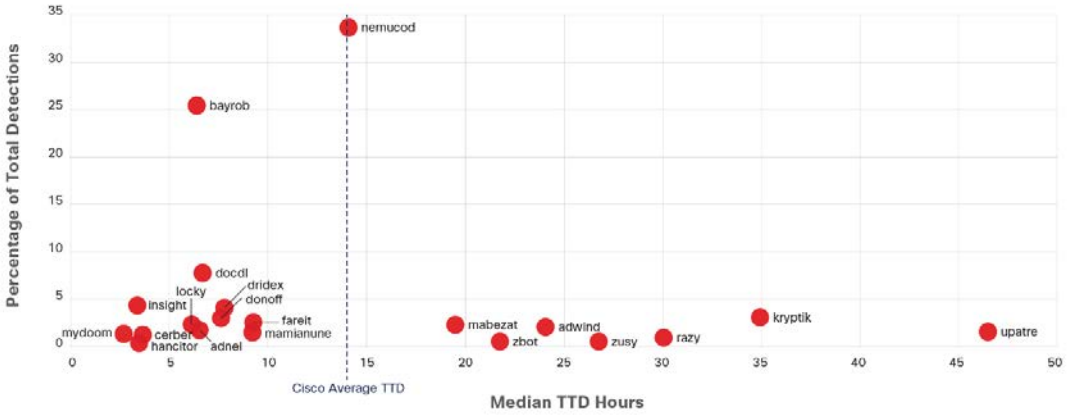
139 Fuente: Microsoft Security Intelligence Report Volume 21 (January through June, 2016). Regional Threat Assessment. (Datos tomados a partir de ordenadores con software MS instalado).

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.4%
2	Win32/Xadupi	Trojans	1.0%
3	Win32/Dynamer	Trojans	1.0%
4	Win32/Skeeyah	Trojans	0.7%
5	Win32/Spursint	Trojans	0.7%
6	Win32/Peals	Trojans	0.6%
7	INF/Autorun	Obfuscators & Injectors	0.6%
8	Win32/Rundas	Trojans	0.5%
9	JS/NeutrinoEK	Exploits	0.4%
10	Win32/Obfuscator	Obfuscators & Injectors	0.4%

Por lo que respecta al código dañino para dispositivos móviles, 2016 ha seguido la tónica de años anteriores: crecimiento. La figura siguiente muestra la evolución de este tipo de software dañino: aparición de nuevas muestras y cifras totales[140].



Finalmente, como en años precedentes, pese al incremento en las contramedidas usadas y su eficacia, uno de los mayores problemas sigue estando en la detección temprana de los ataques por código dañino. La figura siguiente muestra el tiempo medio para la detección de las muestras de código dañino más habituales en 2016, incluyendo el porcentaje de éxito de tal detección[141].



140 Fuente: McAfee Labs, 2016.

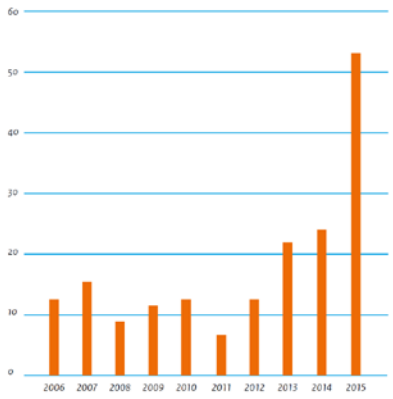
141 Fuente: Cisco Security Report. "2017 Annual Cybersecurity Report".

7.2 Herramientas de los ataques

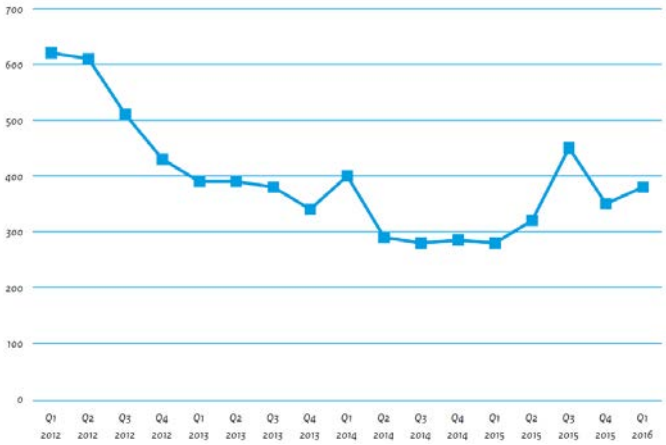
La **comercialización de exploits-kits** sigue siendo una de las amenazas más significativas[142], afectando en la actualidad a ordenadores convencionales, móviles y routers[143]. No obstante, el 86% de los exploits contenidos en exploits-kits aprovechan vulnerabilidades de Flash Player[144].

Como en años precedentes, la comercialización y venta de exploits suele tener lugar tanto en foros underground[145] como a través de campañas comerciales[146], siendo los llamados exploits de día-cero los que alcanzan mayores precios en el mercado negro.

Como se observa en la figura siguiente, el número total de exploits de día-cero conocidos creció significativamente en 2015[147].



La figura siguiente muestra el número de exploits publicados desde 2012[148].



142 Buenos 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).

143 https://github.com/reverse-shell/routersploit

144 https://www2.trustwave.com/rs/815-RFM-693/images/2016%20Trustwave%20Global%20Security%20Report.pdf

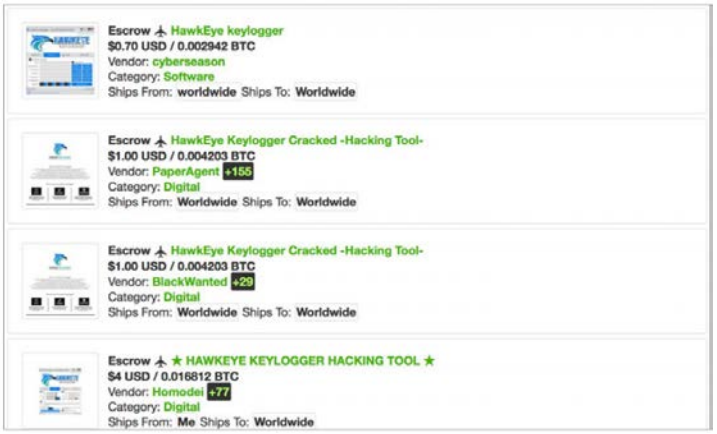
145 http://www.wired.com/2015/04/therealdeal-zero-day-exploits/

146 http://betanews.com/2015/11/20/zerodium-reveals-price-list-for-zero-day-exploits/

147 Fuente: Symantec. Los 54 exploits que muestra la figura, 4 eran de Android, 10 de adobe flash player, 6 de Microsoft Windows, 2 de internet explorer, 2 de Microsoft Office y 10 para software de sistemas de control industrial (véase: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf)

148 Fuente: Exploit-DB.

Por otro lado, las **herramientas de acceso remoto** (*Remote Access Tools*, RAT), sobre diferentes sistemas operativos, continúan constituyendo un procedimiento eficaz para la comisión de distintos tipos de ciberdelincuencia. Además de ello, el bajo coste de adquisición de estas herramientas (5 dólares en foros underground[149]), impulsa su utilización en diferentes entornos. Pueden encontrarse con relativa facilidad varios foros underground que venden -únicamente- herramientas de hacking (keyloggers, herramientas de spam, herramientas de acceso remoto (RAT) y botnets).



En la mayoría de los casos, el código dañino adquirido incluye soporte técnico de sus desarrolladores. Por ejemplo: *Xena RAT Builder*, puede adquirirse bajo dos modalidades: *Silver* o *Gold*. El paquete *Gold* incluye servicios de criptografía para garantizar que el código que se crea sea totalmente indetectable.

Se muestra seguidamente un cuadro con los precios de venta de varios tipos de código dañino[150].

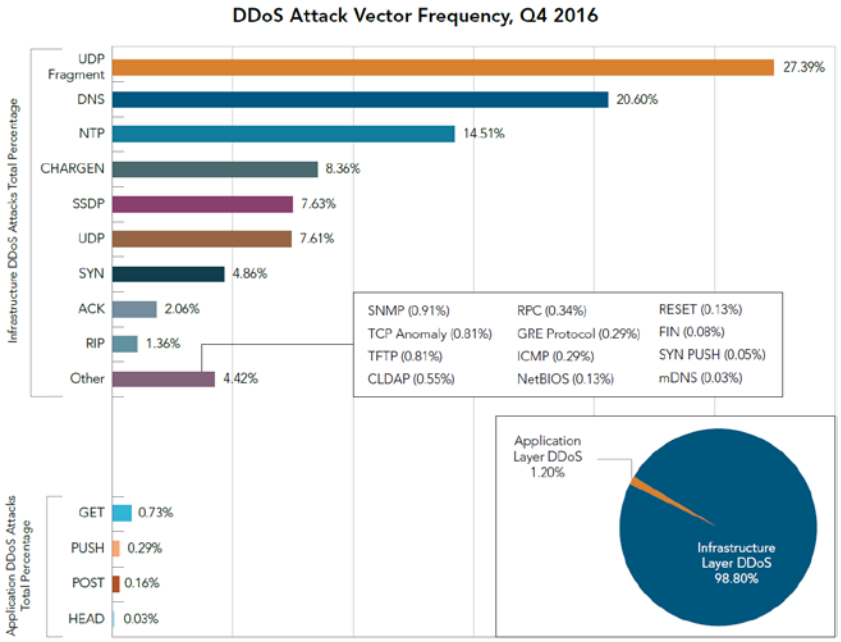
Offering	Price
Keylogger	US$1–4
Xena RAT builder	US$1–50
Exploit	US$1+ (depending on complexity)
Botnet and/or botnet builder	US$5–200
Worm	US$7–15
Ransomware	US$10
Betabot DDoS tool	US$74

149 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

150 Fuente: TrendMicro: North America Underground.

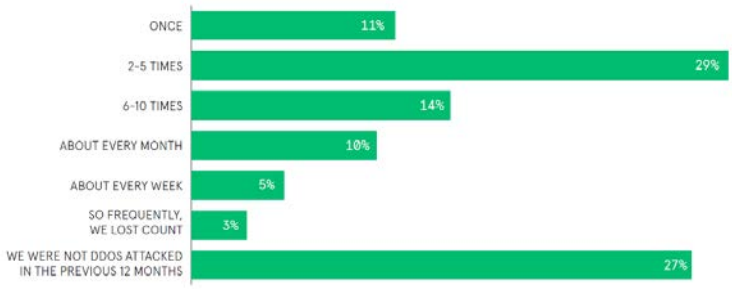
7.3 Ataques de Denegación de Servicio (DoS) y Aplicaciones Web

Según un estudio de Akamai, los ataques DDoS registrados solo en el segundo trimestre de 2016, se incrementaron en un 129% respecto de los registrados en el mismo trimestre de 2015[151]. La figura muestra la frecuencia en el vector de ataque elegido para realizar estas acciones durante el último trimestre de 2016. Además, 2016 ha evidenciado la potenciación de los métodos de amplificación[152].



Las cifras siguientes dan buena muestra de la universalización de los ataques DDoS y sus consecuencias[153]:

- El 73% de todas las organizaciones encuestadas sufrieron un ataque DDoS.
- El 85% de las organizaciones fueron objeto de múltiples ataques DDoS.
- El 44% de las organizaciones atacadas lo fueron seis o más veces.



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

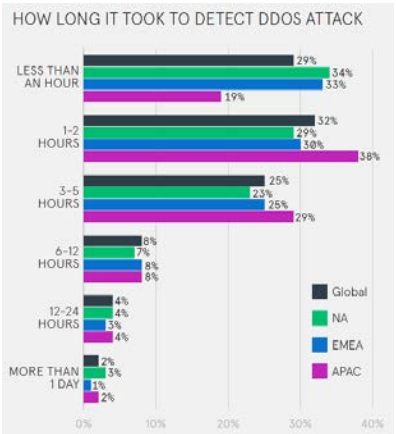
152 Como es sabido, este método consiste en provocar artificialmente peticiones a un sistema cuyas respuestas se convierten también en nuevas peticiones, lo que conduce a colapsar el sistema atacado.

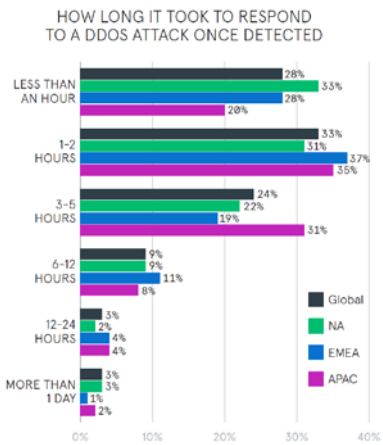
153 Fuente: Encuesta mundial realizada por Neustar: Worldwide DDoS Attacks & Protection Report. Oct., 2016.

- El 49% de los encuestados perdió, al menos, 100.000 dólares por hora durante los períodos punta.
- El 33% perdió, al menos, 250.000 dólares durante los mismos períodos.

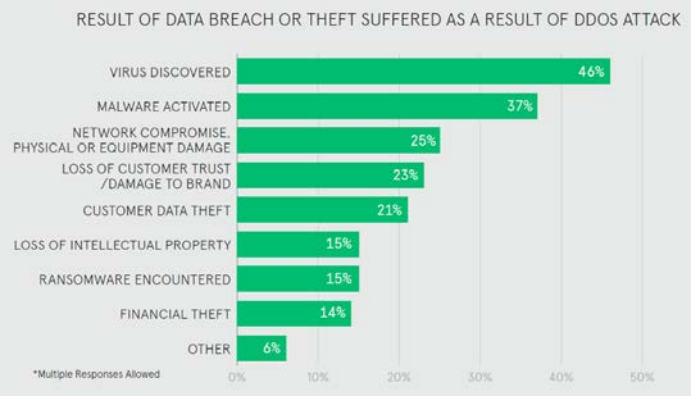
- El 76% de las organizaciones están invirtiendo más mitigación de ataques DDoS.
- El 38% están invirtiendo más en defensas contra ataques DDoS, pero reconocen que la inversión debe ser aún mayor.

- El 39% de los encuestados tardó tres o más horas para detectar un ataque DDoS.
- El 25% detectaron el ataque DDoS entre tres y cinco horas.

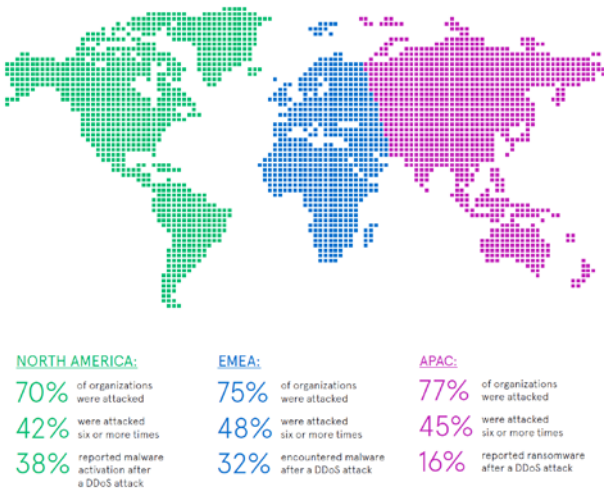




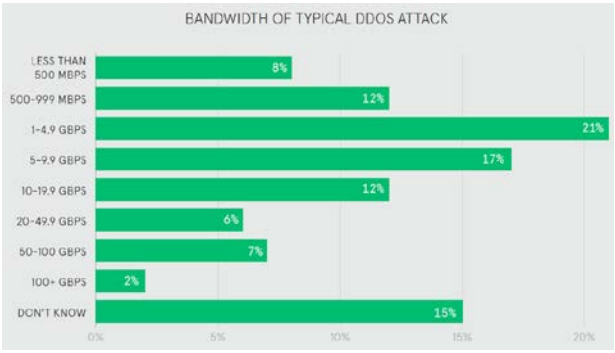
- El 53% de las organizaciones atacadas sufrieron una brecha de datos como resultado de un ataque DDoS.
- El 46% informaron haber encontrado un virus después de la brecha de datos.



La figura siguiente, de la misma fuente, muestra la incidencia de ataques DDoS por continente.



Y su ancho de banda.



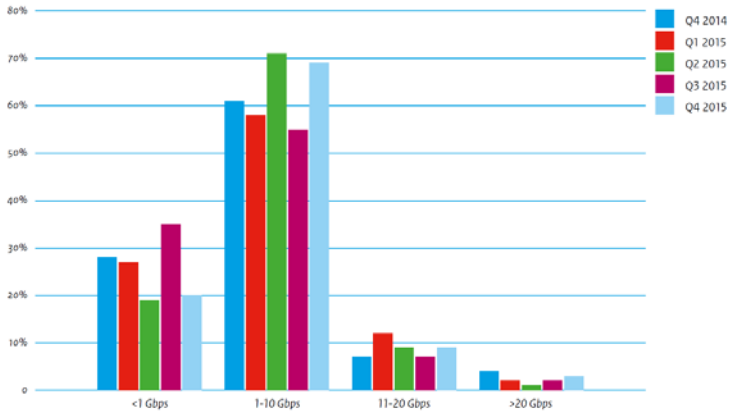
Quizás lo más peligroso de este tipo de acciones es que el nivel de conocimientos que un atacante necesita es muy reducido teniendo en cuenta el significativo número de

websites que están ofreciendo este tipo de servicios de ataque en la modalidad *DDoS-as-a-service.*

Como hemos dicho, durante 2016 se ha continuado buscando nuevas formas de amplificación, tales como las que se han observado abusando de NetBIOS, RPC, Sentinel[154], RPC Portmapper[155], DNSSEC[156], TFTP[157] o Bittorrent[158]. Además de ello, ciertos tipos de dispositivos conectados a internet, tales como routers, cámaras IP, discos duros de red e, incluso, impresoras de red, también se han usado para desarrollar ataques DDoS[159]. Parece razonable esperar que, con el incremento del número de dispositivos (no gestionados) conectados a internet, esta problemática crecerá en los próximos años.

Respecto del tamaño, el volumen y la duración de los ataques DDoS, 2016 ha vuelto a evidenciar un notable crecimiento. Así, el ataque denunciado más significativo comportó 500 gigabits por segundo, aunque ataques de esta magnitud siguen siendo excepcionales. Además de ello, es importante considerar el volumen del ataque, es decir, el número de paquetes por segundo enviados[160], cantidad que es relevante para medir el impacto o de un ataque[161].

La figura siguiente muestra el tamaño de los ataques DDoS detectados en 2016 y 2015[162].



Como puede observarse en la figura anterior, los ataques comprendidos dentro del rango entre 1 y 10 Gbps continúan siendo la mayoría, siendo excepcionales los que se desarrollan con más de 20 Gbps. Asimismo, la mayor parte de estos ataques han sido de

154 https://blogs.akamai.com/2015/10/netbios-rpc-portmap-and-sentinel-reflection-ddos-attacks.html

155 http://blog.level3.com/security/a-new-ddos-reflection-attack-portmapper-an-early-warning-to-the-industry/

156 https://www.stateoftheinternet.com/downloads/pdfs/2016-state-of-the-internet-threat-advisory-dnssec-ddos-amplification-attacks.pdf

157 http://researchrepository.napier.ac.uk/8746/

158 http://arstechnica.com/security/2015/08/how-bittorrent-could-let-lone-ddos-attackers-bring-down-big-sites/

159 Véanse:

http://www.computerworld.com/article/2921559/malware-vulnerabilities/malware-infected-home-routers-used-to-launch-ddos-attacks.html

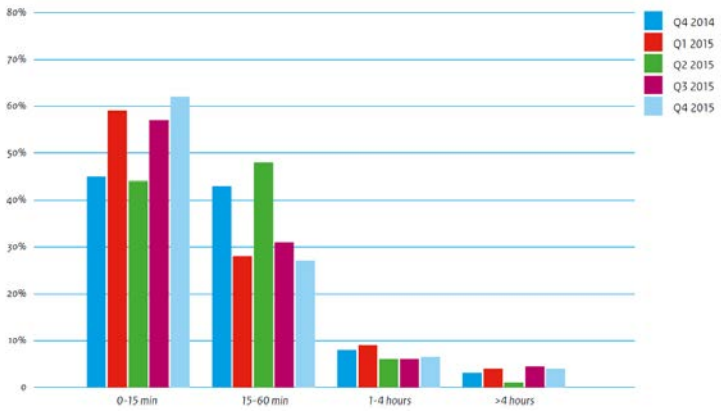
http://www.computerworld.com/article/2996079/internet-of-things/attackers-hijack-cctv-cameras-to-launch-ddos-attacks.html

160 Los ataques con muchos paquetes por segundo requieren más memoria el equipamiento de red. El volumen de los ataques DDoS suele expresarse en millones de paquetes por segundo.

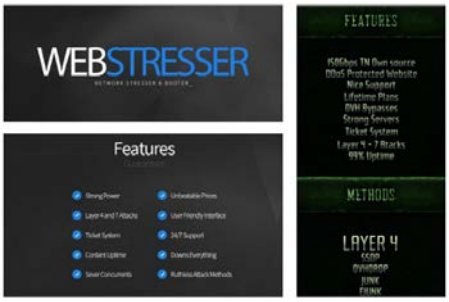
161 https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/2015-q3-cloud-security-report.pdf

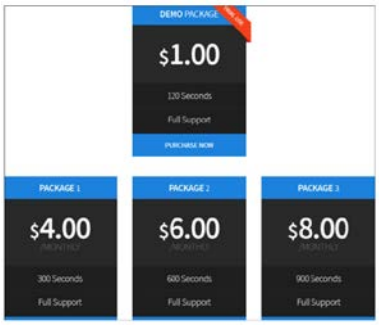
162 Fuente: National anti-DDoS Wash of the National management Organisation of Internet Providers.

corta duración (menores de 15 minutos). Solo en el 10% de los casos los ataques duraron más de una hora, tal y como puede apreciarse en la figura siguiente[163].



Como se ha señalado, también el mercado negro y en los foros underground pueden encontrarse herramientas para perpetrar ataques de este tipo.





Y sus precios[164].

Offering	Price
40GBps for 300 seconds	US$5
70GBps for 300 seconds	US$9
40GBps for 2,700 seconds	US$25
125GBps for 300 seconds	US$25
70GBps for 7,200 seconds	US$30
125GBps for 2,000 seconds	US$60

Finalmente, la figura siguiente muestra la distribución del país de origen de los ataques DDoS, durante 2016[165].

163 Fuente: Idem.

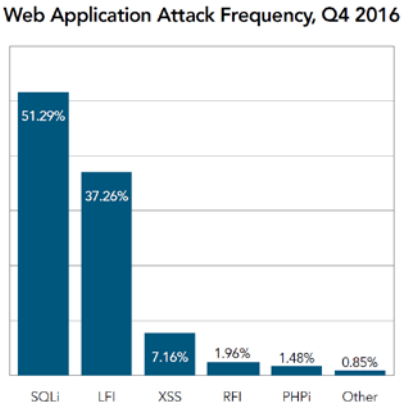
164 Fuente: TrendMicro: North American Underground.

165 Fuente: Akamai's State of the Internet / Security. Q2 a Q4 2016 Report.

Top 5 Source Countries for DDoS Attacks, Q1–Q4 2016

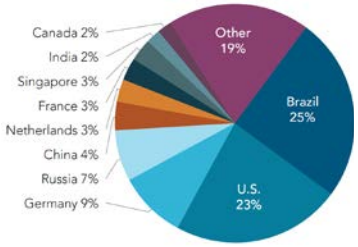
Q1 2016		Q2 2016		Q3 2016		Q4 2016	
Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs
China	16%	China	40%	China	19%	U.S.	24%
	115,478		306,627		81,276		180,652
U.S.	10%	U.S.	12%	U.S.	14%	U.K.	10%
	72,598		95,004		59,350		72,949
Turkey	6%	Taiwan	4%	U.K.	10%	Germany	7%
	43,400		28,546		44,460		49,408
Brazil	5%	Canada	3%	France	6%	China	6%
	36,472		20,601		23,980		46,783
South Korea	4%	Vietnam	3%	Brazil	3%	Russia	4%
	31,692		20,244		13,502		33,211

Por lo que se refiere a **ataques a Aplicaciones Web**, los vectores de ataque más significativos, según la fuente que se cita[166], se muestran en la figura siguiente. Obsérvese la prevalencia de los ataques por inyección SQL y Local File inclusión, frente al resto. Entre ambos se acercan al 90% de la totalidad de los ataques.

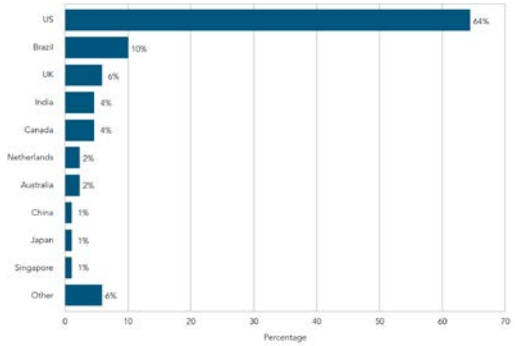


Los cuadros siguientes muestran la distribución por países de origen y destino de tales ataques, en el segundo trimestre de 2016.

Origen de los ataques



Destino de los ataques



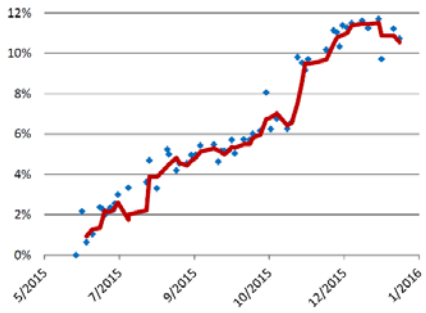
166 Fuente: Akamai's op. cit.

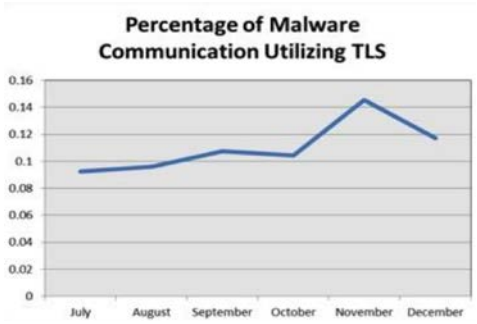
7.4 La ocultación del atacante y el abuso de servicios de buena fe

El interés del atacante es siempre ocultar su verdadera identidad, eliminando, cuando ello es necesario, todas las evidencias que hubiere podido dejar en los sistemas infectados[167].

Por otro lado, en 2016 se ha confirmado el abuso de ciertos servicios muy populares, tales como Dropbox, Pinterest y Google Docs, aprovechando que el tráfico desde o hacia tales servicios suele estar cifrado por defecto. Varios agentes de las amenazas han usado estos servicios para distribuir, de forma inadvertida para sus titulares, código dañino[168].

Sobre la incidencia del cifrado de canales de comunicación, como se ha mencionado en capítulos precedentes, como mecanismo usado por los agentes de las amenazas para ocultar contenido dañino, se ha debatido mucho en 2016 -y seguirá debatiéndose en los próximos años. Un ejemplo: la figura siguiente muestra el incremento del uso de canales SSL (izquierda)[169] y el porcentaje de uso de TSL para comunicar código dañino (derecha)[170].





No cabe duda que el uso de SSL y TLS seguirá aumentando en todo el mundo, al tiempo que resulta previsible asimismo el aumento del volumen de código dañino avanzado y los casos de robo de datos usando SSL/TLS. Todo ello significa que la gestión del tráfico cifrado (ETM) está llamada a jugar un papel cada vez más importante en la protección de las infraestructuras. Sin embargo, las organizaciones -públicas y privadas- necesitan encontrar soluciones ETM capaces de satisfacer también las exigencias

167 Algunos ejemplos de ello son los denominados USBthief, en los que el código dañino que contienen sólo puede ejecutarse desde el pen drive original, sin dejar ninguna evidencia en el sistema comprometido (véase: http://www.welivesecurity.com/2016/03/23/new-self-protecting-usb-trojan-able-to-avoid-detection/) o el código dañino Cherry Picker, específicamente diseñado para sistemas POS, y que contiene elementos de auto-limpieza de evidencias una vez alcanzados sus objetivos (véase: https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/). En otros casos, el código dañino opta por borrar completamente el disco duro una vez desarrollado el ataque, eliminando por consiguiente todas las evidencias (véase: http://blogs.cisco.com/security/talos/rombertik). Finalmente, se han encontrado otros casos de código dañino que trabajan exclusivamente en la memoria del equipo de la víctima, tal como Duqu 2.0, por ejemplo (véase: https://cdn.securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf).

168 Por ejemplo, Hamertoss, la puerta trasera del grupo denominado APT29, usó Twitter para comunicarse con sus sistemas C&C (véase: https://www.fireeye.com/blog/threat-research/2015/07/hammertoss_stealthy.html). Asimismo, dos familias de código dañino para Android (OpFake y Marry) usaron Facebook como infraestructura C&C (véase: http://news.softpedia.com/news/two-mobile-banking-trojans-used-facebook-parse-as-c-c-server-497597.shtml). Por el mismo propósito o , el grupo chino denominado admin@338 utilizó cuentas de Dropbox (véase: http://news.softpedia.com/news/malware-that-hides-c-c-server-on-dropbox-detected-in-the-wild-496951.shtml).

169 Fuente: Universidad de Michigan: Increase in SSL servers on port 443 in the global IPv4 Internet.

170 Fuente: Cisco Systems Inc.: "Hiding in Plain Sight: Malware's Use of TLS and Encryption," Enero, 2016. (Véase: http://blogs.cisco.com/security/malwares-use-of-tls-and-encryption).

derivadas de la privacidad de los datos, la compatibilidad, la seguridad, el rendimiento, la escalabilidad y la rentabilidad, todo en igual medida.

Por si fuera poco, los atacantes también abusaron de autoridades de certificación legítimas para obtener certificados digitales con los que aparentar una imagen de legalidad[171], así como de comunicaciones vía satélite para enmascarar la localización de los servidores C&C[172].

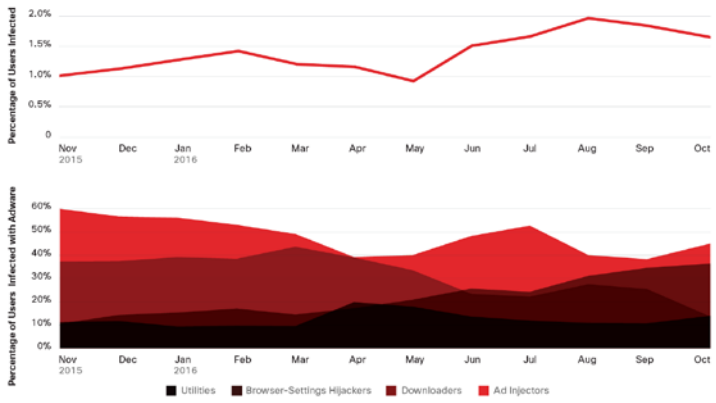
Ante esta realidad, las fuerzas policiales de muchos países han insistido en disponer de mecanismos que permitan el descifrado de información cifrada cuando existan sospechas fundadas de que se están cometiendo acciones criminales al socaire de dicho cifrado.

7.5 La publicidad dañina

La publicidad dañina -aquella que se utiliza para infectar los ordenadores de la víctima- continúa siendo muy usada por los agentes de las amenazas.

Muchas páginas web utilizan redes especializadas en publicidad, así como agentes publicitarios, que introducen mensajes comerciales en sus infraestructuras. Si tales mensajes comerciales han sido previamente infectados cualquier usuario que tenga acceso a dicha publicidad podrá infectarse con código dañino.

La figura siguiente muestra un gráfico con el desglose de los incidentes de 2016 atendiendo al componente usado por la publicidad dañina (adware dañino)[173].



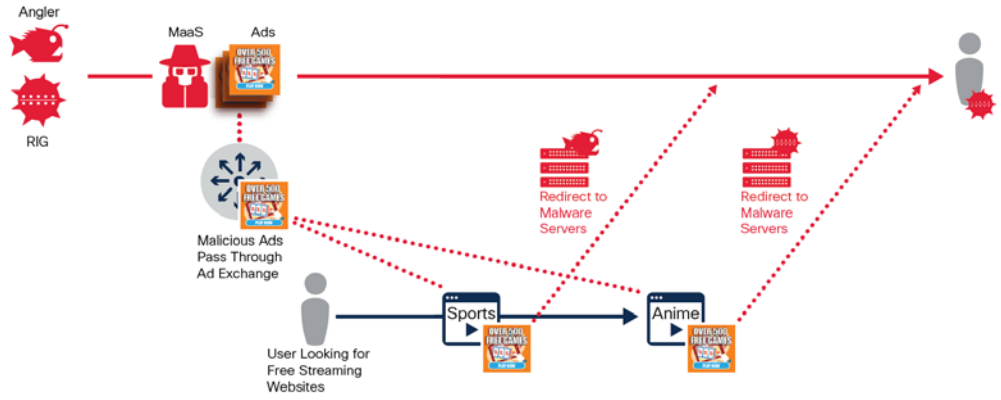
La figura siguiente muestra la evolución de este tipo de amenazas, al llamado Malvertising-as-a-service (MaaS), y cómo se ha llevado a cabo en 2016[174].

171 Tal fue el caso, por ejemplo, de los certificados de la iniciativa Let's Encrypt, que también fueron usados para securizar una página web de Phishing.

172 Tal como se hizo con los ataques de exfiltración de datos del grupo TURLA.

173 Fuente: Cisco Security Research. "2017 Annual Cybersecurity Report".

174 Fuente: Cisco Security Research.



Si pensamos que determinadas páginas web reciben diariamente cientos de miles de visitas, concluiremos en 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 ad-blockers.

8. MEDIDAS

Analizados los agentes de las amenazas, sus métodos y las vulnerabilidades atacadas, en los siguientes epígrafes se muestran aquellas medidas que, por su novedad, eficacia o singularidad, han resultado más significativas en 2016.

8.1 El factor humano

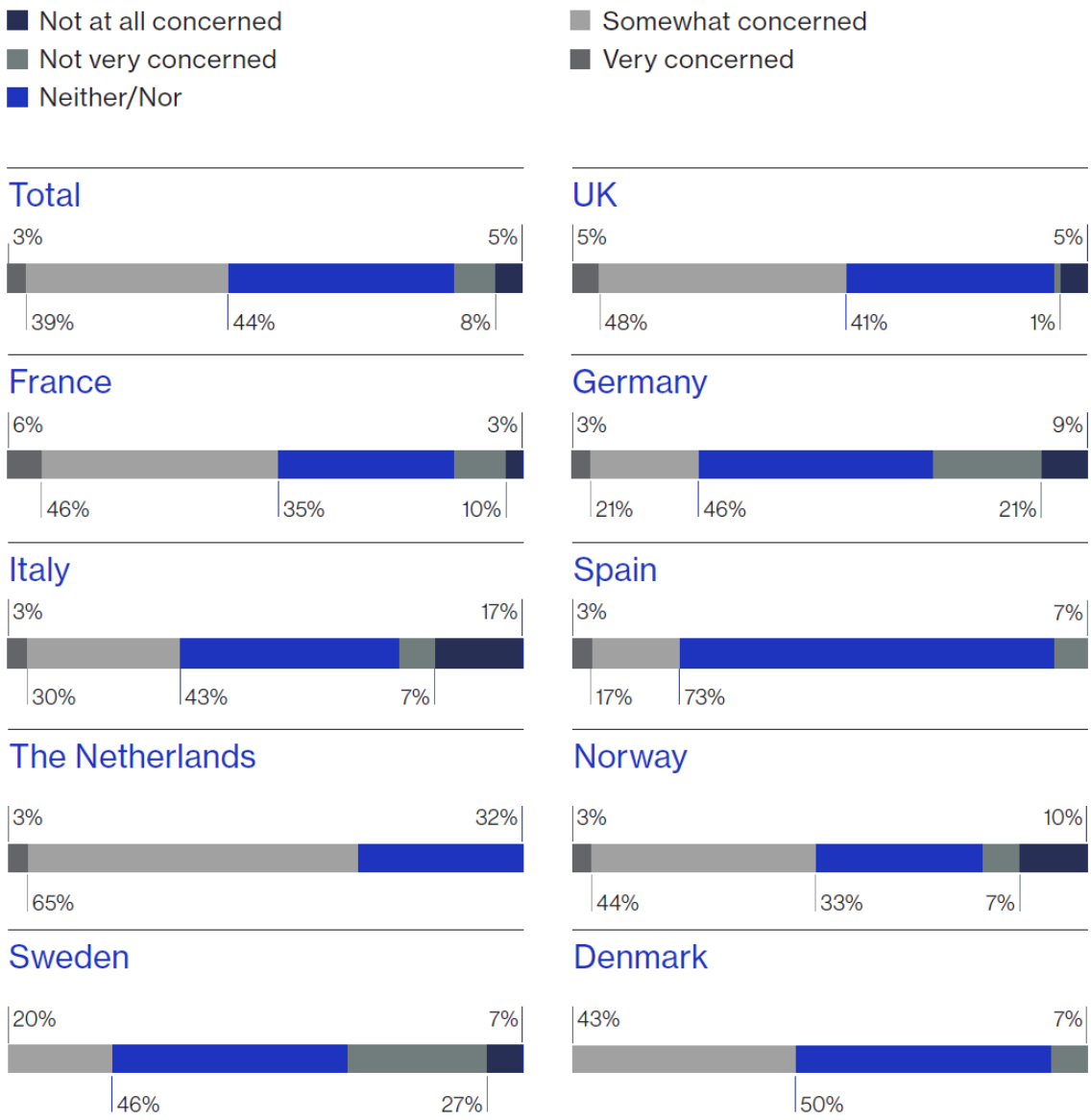
Tras las revelaciones de Snowden y Wikileaks, son muchas las organizaciones -públicas y privadas- preocupadas por ataques con origen en los estados[175]. La preocupación por la **privacidad** de los datos personales tuvo como consecuencia que, en octubre 2015, el Tribunal de Justicia de la Unión Europea declarará inválido el Acuerdo de Puerto Seguro, que tuvo que ser sustituido, en julio de 2016, por el denominado Escudo de Privacidad (*Privacy Shield*), que regula actualmente el intercambio de datos personales entre la Unión Europea y los Estados Unidos[176].

Pese a la constante aparición de noticias, la concienciación en materia de ciberseguridad sigue siendo una asignatura pendiente en muchos países. La figura siguiente, proveniente de una encuesta realizada por Lloyd's, muestra el grado de concienciación de los empresarios de ciertos países europeos[177] sobre tales extremos.

175 Algunas organizaciones, como Facebook, Google y otras, ya están advirtiendo a los usuarios si se sospecha de un ataque originado en un estado (véase: http://www.securityweek.com/microsoft-warn-users-state-sponsored-attacks,).

176 http://europa.eu/rapid/press-release_IP-16-2461_en.htm

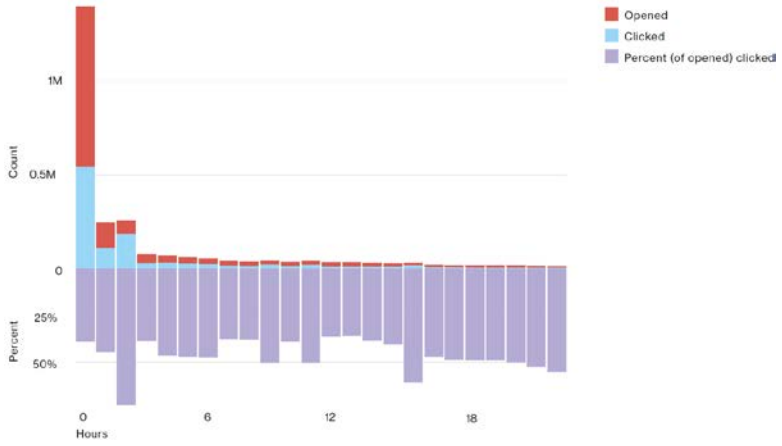
177 Fuente: Lloyd's: Facing the Cyber Risk Challenge, (Sep., 2016). Sobre una muestra de 346 empresarios europeos, repartidos del siguiente modo: UK (100), Francia (31), Alemania (34), Italia (30), España (30), Países Bajos (31), Noruega (30) y Dinamarca (30).



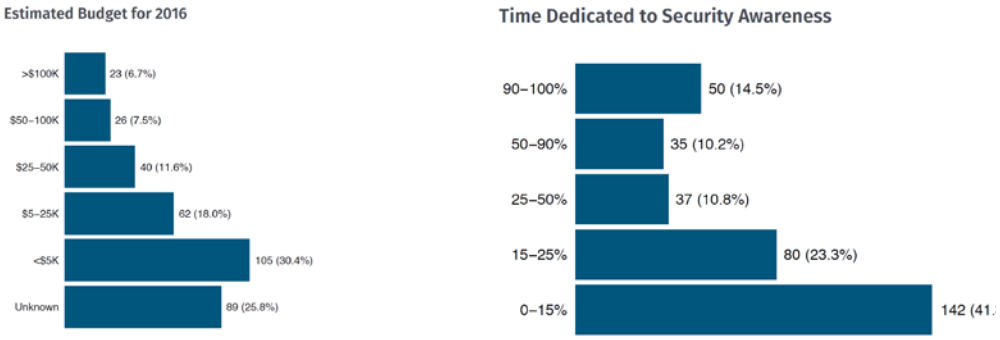
Esta realidad ha ido acompañada en los últimos años de diferentes iniciativas y campañas en favor de la **sensibilización y concienciación** de los usuarios. Así, nos hemos encontrado con el *Mes Europeo de la Ciberseguridad* y otras iniciativas nacionales. Pese a todo, un reciente informe de Verizon[178] señala claramente que la sensibilización, por sí sola, no es suficiente. De acuerdo con este informe, los usuarios abren el 30% de los correos electrónicos de phishing, y el 12%, además, abren asimismo los ficheros adjuntos[179].

178 Verizon: "2016 Data Breach Investigations Report".

179 Con una particularidad añadida: el receptor abrió el adjunto en los cuatro minutos siguientes al envío del correo electrónico dañino (véase: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/).



Dos de los mayores inconvenientes que deben afrontar los equipos de las organizaciones dedicados a la concienciación es la escasez de presupuesto, así como una dedicación temporal muy limitada. La figura siguiente muestran datos reales sobre ambas problemáticas[180].



Atendiendo a los resultados observados en 2016, y pese a que la concienciación en materia de ciberseguridad está todavía en su infancia, están empezando a aparecer los primeros signos de madurez. Las organizaciones -públicas y privadas- parecen estar recibiendo un poco más de apoyo que en años anteriores, observándose una mejora en el nivel medio: está empezando a lograrse una mejor comprensión de cuáles son los retos principales y cómo abordarlos mejor.

Por otro lado, muchas instituciones señalan como una verdadera amenaza la actual escasez de profesionales (técnicos y jurídicos) en materia de seguridad de la información[181]. Parece necesario, por tanto, el desarrollo de programas formativos,

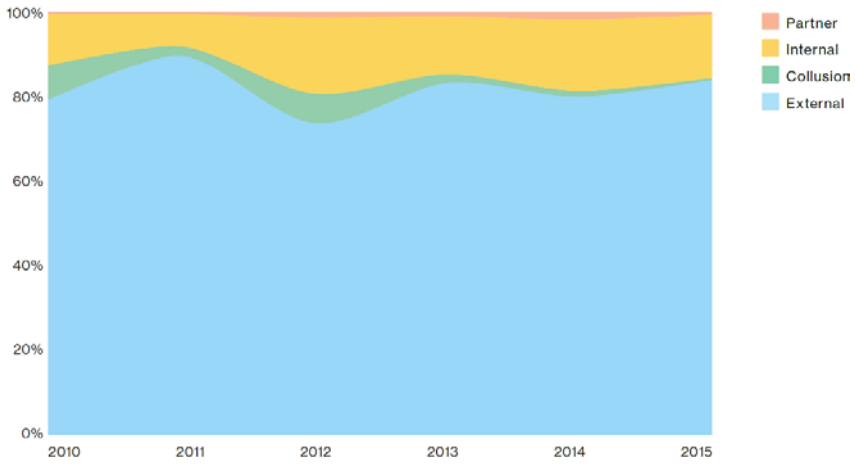
180 Fuente: SANS, atendiendo a una encuesta iniciada en Noviembre de 2015, sobre un total de 369 encuestados de todo el mundo, de 18 sectores. (Awareness Is Hard: A Tale of Two Challenges, 2016).

181 En la actualidad, se estima que más de 209.000 puestos de trabajo relacionados con la ciberseguridad están vacantes sólo en los Estados Unidos, estando previsto que este número aumentará a 1,5 millones en 2019. (Fuente: Steve Morgan, "One Million Cybersecurity Job Openings in 2016," Forbes, January 2, 2016, http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#5e7e881d7d27).Desde el gobierno federal hasta los miembros de Fortune 500, se espera que la demanda de estos profesionales -formados y experimentados- aumente en los próximos años, especialmente a medida que las organizaciones continúen sufriendo brechas de datos y otras ciberamenazas cibernéticas. La escasez de profesionales de la ciberseguridad se ve exacerbada por la falta de claridad y coherencia en los modelos de competencia, descripciones de puestos, certificaciones profesionales y formación y educación, lo que dificulta identificar, reclutar, ubicar y administrar adecuadamente los profesionales que las organizaciones necesitan (Fuente: "Understanding Cyber threats", Sept-2016, Francesca Spidalieri, Pell Center - Salve Regina University).

especialmente dirigidos a tecnólogos y juristas, capaces de construir una población de profesionales cualificados en Ciberseguridad y Ciberdefensa[182].

Esta necesidad queda claramente reflejada en la figura siguiente, tomada de una encuesta realizada por la empresa norteamericana SalesForce, sobre 2.200 encuestados de todo el mundo[183], en la que la necesidad de especialistas en seguridad IT aparece como la segunda prioridad de las entidades para los próximos años.

Finalmente, señalar que, pese a todo, la mayoría de las amenazas no provienen de la acción directa de **actores internos**. La figura siguiente muestra el porcentaje de brechas de seguridad, atendiendo a su autor[184].



8.2 El factor tecnológico

Pese a que, como se viene repitiendo, el comportamiento del usuario constituye en muchas ocasiones el eslabón más débil de la cadena de la ciberseguridad, la tecnología sigue siendo indispensable para garantizarla.

Uno de los elementos más delicados lo constituyen sin duda alguna las **versiones más antiguas** del software de base[185].

182 Merece especial atención destacar la presencia cada vez mayor de profesionales del Derecho (nacional, europeo e internacional) en los ámbitos de la ciberseguridad. En la actualidad, el adecuado tratamiento de los riesgos, las amenazas la identificación de sus autores y las respuestas requeridas, exigen la formación de equipos multidisciplinares en los que se ven involucrados tanto tecnólogos como juristas.

183 Fuente: SalesForce: 2016 State Of IT.

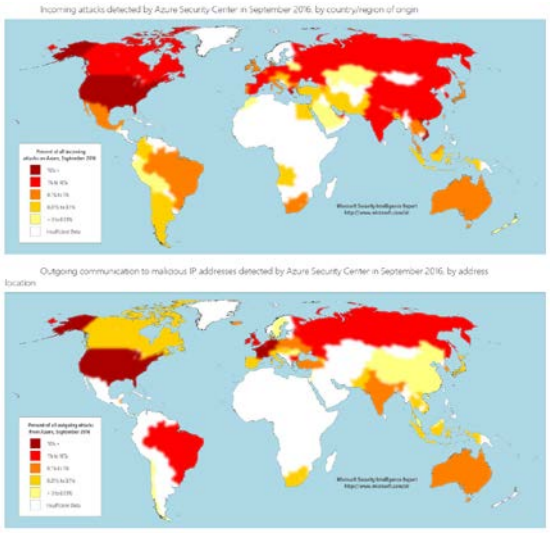
184 Fuente: Verizon: 2016 Data Breach Investigations Report.

185 Un ejemplo: durante 2015 Microsoft una campaña para animar a los usuarios a descargar sin coste Windows 10, esperando que con ello se reemplazarían versiones antiguas de este sistema operativo. Pese a las indudables ventajas de Windows 10, Windows 7 continúa siendo el sistema operativo más extendido (véase: http://gs.statcounter.com/#desktop-os-ww-monthly-201503-201603316)

Pese a que la mayoría de las organizaciones consideran necesario adoptar una serie de medidas mínimas de seguridad, no parece existir un consenso respecto o de qué medidas serían las más idóneas para prevenir ataques. La **utilización de estándares** puede ayudar de manera significativa a encontrar tales medidas[186].

La **externalización de servicios TIC** -muy especialmente los llamados *Servicios en la nube*- sigue siendo una tendencia en aumento por parte de todo tipo de organizaciones, públicas y privadas. Un buen ejemplo de ello lo constituyen los servicios de correo electrónico centralizados. Este tipo de servicios en la nube, cuando son prestados por proveedores de reconocido prestigio, suelen disponer de medidas de seguridad más efectivas que las que podrían adoptarse en una organización particular[187].

Como se muestra en la figura siguiente[188], y atendiendo a las fuentes consultadas, la utilización de servicios en la nube reduce significativamente el riesgo de sufrir un ciberataque o, en el peor de los casos, que tenga éxito. Por este motivo es especialmente importante el uso de **nubes privadas** en aquellos ambientes que deseen beneficiarse de las ventajas de su utilización, sin menoscabo de seguridad, como es el caso, por ejemplo, de las entidades del sector público.



No obstante, lo anterior, el uso de servicios en la nube comporta un riesgo adicional de ciberespionaje. Una brecha de seguridad en el software usado por un prestador de servicios en la nube (PSC) puede tener consecuencias inmediatas y desastrosas para todos sus clientes[189].

Como hemos señalado, los **ataques por DDoS**, que siguen constituyendo una de las amenazas más significativas, pueden limitarse configurando adecuadamente los

186 Tales como ISO 27000, por ejemplo.

187 Por ejemplo, el uso de SPF para todos los clientes de un determinado proveedor.

188 Fuente: Microsoft Security Intelligence Report. Volume 21 | January through June, 2016.

189 Por ejemplo, en enero de 2016, dos investigadores encontraron una vulnerabilidad en Microsoft Office 365 que posibilitaba la penetración en cuentas de otras organizaciones (véase: https://bratec.si/security/2016/04/27/road-to-hell-paved-with-saml-assertions.html)

routers de las organizaciones, con lo que se detiene la entrada de paquetes falsos[190]. La figura siguiente muestra una relación de las medidas más usadas en 2016 contra ataques DDoS[191].

La necesidad -manifestada en muchas ocasiones- de las Fuerzas y Cuerpos de Seguridad por **acceder a comunicaciones cifradas** está provocando una significativa confrontación entre aquellos que predican el derecho a la privacidad por encima de cualquier otra consideración y la citada necesidad policial y de inteligencia por disponer de herramientas que permitan atajar los comportamientos delictivos en el ciberespacio.

Así, en setiembre de 2015, el gobierno o de los Estados Unidos intentó persuadir a determinadas empresas públicas para cooperar en el campo del cifrado y descifrado de información[192], sin demasiado éxito. En marzo de 2016, la confrontación llegó al FBI, mediante una demanda judicial, para conseguir la ayuda de Apple para acceder a un teléfono incautado a un terrorista[193]. Apple, alegando que esta concesión podría afectar a la totalidad de sus clientes, no estuvo de acuerdo en facilitar tal acceso[194].

En el fragor de la batalla, WhatsApp anunciaba la comunicación cifrada extremo a extremo para todos sus usuarios[195] abordando la realidad de que el cifrado de la información -incluso en tránsito- sigue percibiéndose por los usuarios como una garantía adicional de su derecho a la privacidad. En junio de 2015 el gobierno norteamericano decidió que todas las páginas web de los departamentos gubernamentales se desarrollarían usando https[196]. Por otro lado, el lanzamiento de Let's Encrypt, públicamente disponible a finales de 2015, ayudó a avanzar en la adopción del protocolo https y el cifrado de información.

Pese a todo, el compromiso de las autoridades públicas con el derecho de los usuarios a cifrar su información ha sido puesto de manifiesto en 2016 por varios gobiernos occidentales[197].

190 http://www.routingmanifesto.org/

191 Fuente: NeuStar. Op. Cit.

192 http://motherboard.vice.com/read/the-white-house-thinks-it-can-make-a-deal-with-companies-to-break-encryption

193 https://assets.documentcloud.org/documents/2714001/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf

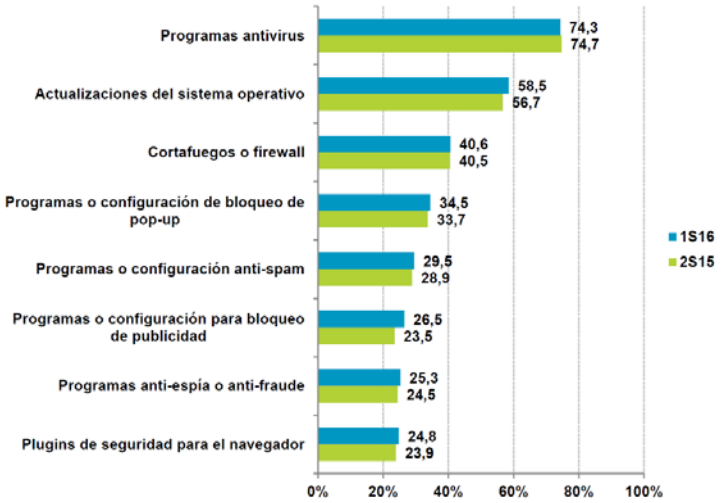
194 http://www.apple.com/customer-letter/

195 https://blog.whatsapp.com/10000618/end-to-end-encryption

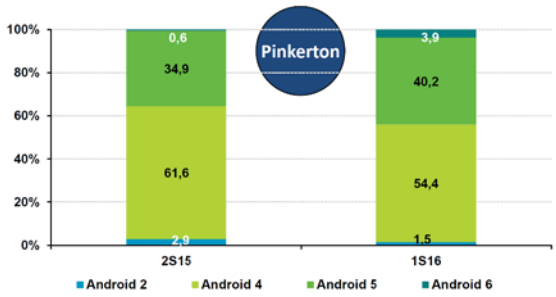
196 https://https.cio.gov/

197 Entre ellos, el holandés y el francés.

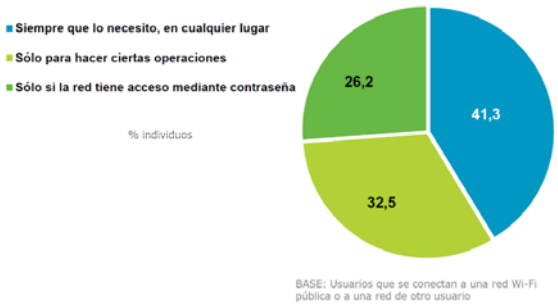
Por lo que respecta a los ciudadanos españoles, la figura siguiente muestra el uso de las principales **medidas de seguridad automatizables,** que se mantiene estable con respecto al estudio anterior[198].



Respecto de los **dispositivos móviles** usados por los ciudadanos, la figura siguiente muestra la distribución de las diferentes versiones de Android[199].



Respecto del uso de Wi-Fi fuera del perímetro de seguridad (domicilio, oficina, etc.), la figura siguiente muestra una realidad preocupante: el 41,3% de usuarios españoles que se conecta a una red inalámbrica Wi-Fi pública lo hace siempre que lo necesita y en cualquier lugar, exponiendo, por consiguiente, la confidencialidad e integridad de sus datos a los riesgos de operar en redes no protegidas.



198 Fuente: ONTSI: Estudio sobre la Ciberseguridad y la confianza en los hogares españoles. Junio, 2016.

199 Fuente: ONTSI. Op. Cit.

8.3 El factor económico y metodológico

A medida que el ciberespacio se va integrando en la vida diaria, también se van planteando nuevos riesgos y amenazas para los ciudadanos, empresas y Administraciones, de diversa naturaleza e impacto. Cada día se plantean nuevos peligros cibernéticos que difícilmente se pueden cuantificar mediante ejercicios prospectivos. Es en este contexto donde las **pólizas de ciberriesgos**[200] se erigen como medidas de 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. Tales pólizas no sólo permiten gestionar los ciberriesgos corporativos con mayor efectividad que hasta ahora y mejorar el nivel general de la ciberseguridad industrial, sino que también aportarán a las organizaciones un conocimiento relevante de las ciberamenazas[201].

La figura siguiente muestra la distribución de siniestros y reclamaciones por sector, más habituales[202].

Finalmente, 2016 ha colocado en el panorama mundial de la lucha contra las ciberamenazas la llamada **Defensa Activa**. Las medidas de defensa activa incluyen aquellas que, típicamente, van a más allá de una respuesta defensiva a los ciberataques. 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. Tales acciones, tomadas como respuesta a la consecución de objetivos ofensivos, afectan la confidencialidad, integridad o accesibilidad de los datos de otras partes, distintas de la víctima. Ya no son de naturaleza pasiva, y su caracterización depende de la intención o el objetivo del actor que las implementa. Así, por ejemplo, la interrupción de una red

200 Hoy en día, el negocio de los ciberseguros es una industria de 3 mil millones euros, con más del 95%o de todas las pólizas de ciberseguro suscritas en el mundo originadas en los Estados Unidos. Los expertos del mercado estiman que la industria se triplicará en tamaño en 2020 estando en cerca de 8-9 mil millones de dólares, y que continuará creciendo exponencialmente. (Fuente: Matt Cullina, "Cyber Liability Insurance," presentation delivered at the Executive Seminar: Understanding Cyber Threats in the Boardroom, Providence, May 4, 2016).

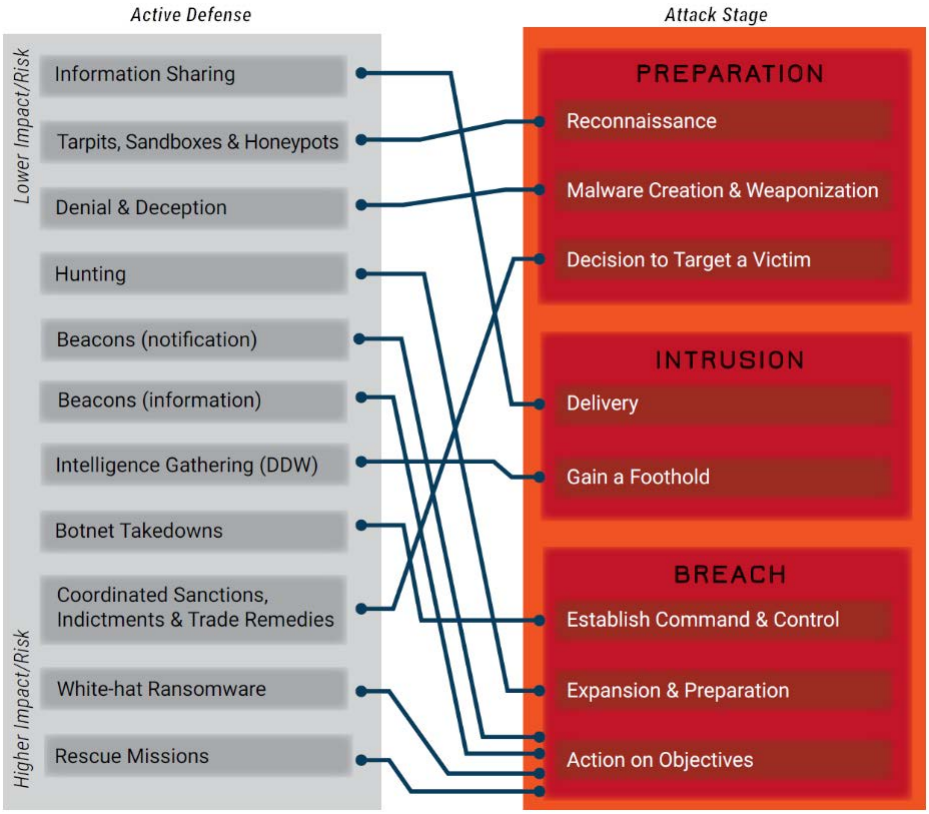
201 Thiber: Ciberseguros: la transferencia del ciberriesgo en España (2016).

202 Fuente: Net Diligence: 2015 Cyber Claims Study, Gladwyne: Network Standard Corporation.

32 Thiber.

de bots, el ataque a un servidor de mando y control o la destrucción de tráfico de una dirección IP atacante son actividades realizadas en respuesta directa a una amenaza.

La figura siguiente muestra el repertorio habitual de medidas de Defensa Activa tendentes a bloquear un ciberataque[203].



8.4 Iniciativas internacionales

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

La exportación de software de intrusión: como es sabido, en 2013, diferentes tecnologías y herramientas relacionadas con software de intrusión se añadieron al Acuerdo de Wassenaar sobre tecnologías de doble uso. En el verano de 2015, el gobierno norteamericano lanzó una consulta pública en relación con este asunto, en el la que se evidenció que el concepto "software de intrusión" debe ser mejor definido[204].

La Directiva Europea NIS: en julio de 2016, el Parlamento Europeo adoptó la Directiva sobre seguridad de las redes y los sistemas de información, otorgando a los estados-miembro veintiún meses para trasponer su contenido a los ordenamientos jurídicos nacionales, incluyendo un plazo adicional de seis meses para designar operadores de servicios esenciales. La Directiva Europea exige a todos los estados

203 Fuente: Center for Cyber & Homeland Security. The George Washington University: Into the Gray Zone. The Private Sector and Active Defense against Cyber Threats (Oct., 2016).

204 https://threatpost.com/security-researchers-sound-off-on-proposed-us-wassenaar-rules/113023/

disponer de capacidades propias en materia de ciberseguridad, fortaleciendo la cooperación entre estados y estableciendo requisitos específicos para los operadores de servicios esenciales.

El Reglamento General de Protección de Datos (RGPD): El 27 de abril de 2016, se publicó el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Como así se ha dicho, esta regulación europea, que será de plena aplicación en mayo de 2018, dibuja un elemento esencial: la que puede denominarse como "responsabilidad activa"; esto es, la obligación de las organizaciones de anticiparse a los ciberincidentes -accidentales o deliberados- que razonablemente pudieran ocurrir, haciendo uso de una metodología que conduzca a la adopción de un conjunto de medidas adecuadas que aseguren -también, razonablemente- que están en condiciones de cumplir con los principios, derechos y garantías que el RGPD establece.

El despliegue de CSIRT en el mundo: Un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) se define habitualmente como un equipo o una entidad -dentro de una agencia u organismo que lo alberga- que proporciona servicios y apoyo a un grupo particular (la comunidad de destino) con el fin de prevenir, gestionar y responder a los incidentes de seguridad de la información. Estos equipos están compuestos generalmente por especialistas multidisciplinares que actúan de acuerdo con los procedimientos y políticas predefinidos para responder rápida y eficazmente a los incidentes de seguridad y para reducir el riesgo de ciberataques.

Hay cientos de CSIRT en el mundo, con distintas misiones y alcances. Una de las principales formas de clasificar a los CSIRT es agruparlos por el sector o por la comunidad a los que sirven. En 2016, el número de equipos adscritos a FIRST[205] era de 369, de 80 países distintos, entre ellos 14 de España.

La revelación responsable de vulnerabilidades: partiendo de determinadas iniciativas *nacionales, muchas organizaciones están empezando a adoptar modelos de* "Revelación Responsable y Coordinada de Vulnerabilidades", como el mecanismo más adecuado para conciliar la actividad de los ciberinvestigadores con la necesaria discreción de los hallazgos encontrados[206]. En abril de 2016, la International Standardisation Organisation (ISO) publicó el documento uno ISO 29147 sobre revelación de vulnerabilidades[207].

En febrero de 2016, la administración norteamericana anunció el **Plan de Acción Nacional de Ciberseguridad (*Cibersecurity National Action Plan- CNAP*),** contemplando nuevas medidas y fomentando las condiciones necesarias para conseguir mejoras a

205 Principal organización de CSIRT del mundo https://www.first.org

206 Así, por ejemplo, la compañía General Motors anunció en 2016 un programa de revelación responsable de vulnerabilidades en todos sus productos. Lo mismo ha sucedido con varias líneas aéreas, que están premiando con "millas" a aquellos que les informen de vulnerabilidades. Google ha llegado a pagar más de dos millones de dólares en 2015 en este tipo de actividad (véase: https://googleonlinesecurity.blogspot.nl/2016/01/google-security-rewards).

207 http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

largo plazo, tanto en el sector público como en el privado y en los ciudadanos. Entre los más aspectos destacados del CNAP se incluyen las siguientes acciones:

- Establecer la "Comisión para el Fortalecimiento de la Ciberseguridad Nacional", que se encargará de formular recomendaciones sobre las medidas que pueden adoptarse en el próximo decenio para reforzar la ciberseguridad tanto en el sector público como en el privado, protegiendo al mismo tiempo la privacidad; mantener la seguridad (pública, económica o nacional); fomentar la investigación y el desarrollo de nuevas soluciones; y fortalecer las alianzas entre los gobiernos federal, estatal y local y el sector privado, en el desarrollo, promoción y uso de tecnologías, políticas y mejores prácticas en materia de ciberseguridad.
- Modernizar los sistemas TIC gubernamentales y transformar la forma en que el Gobierno administra la ciberseguridad a través de la propuesta de un Fondo de Modernización de la Tecnología de la Información de 3.100 millones de dólares, que permitirá el desmantelamiento, reemplazo y modernización de las TIC heredadas, difíciles de securizar y caras de mantener, incluyendo la creación de un nuevo cargo, el Oficial Federal de Seguridad de la Información, para impulsar estos cambios en todo el Gobierno.
- Sensibilizar a los estadounidenses para asegurar sus cuentas en línea moviéndose más allá de las contraseñas y añadiendo una capa adicional de seguridad, tales como huellas dactilares o códigos de un solo uso, mediante la autenticación por múltiples factores, que será la idea central para una nueva Campaña Nacional de Concienciación en Ciberseguridad, organizada por la National Cybersecurity Alliance, que contará con partners como Google, Facebook, DropBox y Microsoft y compañías de servicios financieros como MasterCard, Visa, PayPal y Venmo. Además, el Gobierno Federal tomará medidas para salvaguardar los datos personales en las transacciones en línea entre los ciudadanos y el gobierno.
- Invertir más de 19 mil millones de dólares para la ciberseguridad, como parte del Presupuesto del Año Fiscal del Presidente para 2017. Esto representa un aumento de más del 35% respecto de 2016.

También es importante señalar que, en abril de 2016, el Departamento de Estado norteamericano presentó al Congreso la ***International Cyberspace Policy State,*** que incluye un informe sobre el trabajo del Departamento para implementar la ***President's 2011 International Strategy for CyberspacePlan,*** así como una relación de los esfuerzos para promover normas de comportamiento responsable de los estados en el ciberespacio, conceptos alternativos para las normas promovidas por otros países, amenazas a las que se enfrentan los Estados Unidos, herramientas disponibles para disuadir a los atacantes y los recursos necesarios para construir normas internacionales.

En julio de 2016, se publicó en Estados Unidos la ***Presidential Policy Directive (ppd-41): United States Cyber Incident Coordination.*** Esta Directiva Presidencial establece los principios que rigen la respuesta del Gobierno Federal a cualquier ciberincidente, tanto cuando involucre a entidades del gobierno como del sector privado. En el caso de ciberincidentes significativos, la Directiva Presidencial señala las agencias

gubernamentales que dirigirán la respuesta, así como una arquitectura para coordinar ésta en el gobierno federal. La Directiva exige a los Departamentos de Justicia y Seguridad Nacional mantener la información de contacto actualizada para uso público, y así ayudar a las entidades afectadas por ciberincidentes a reportarlos a las autoridades competentes.

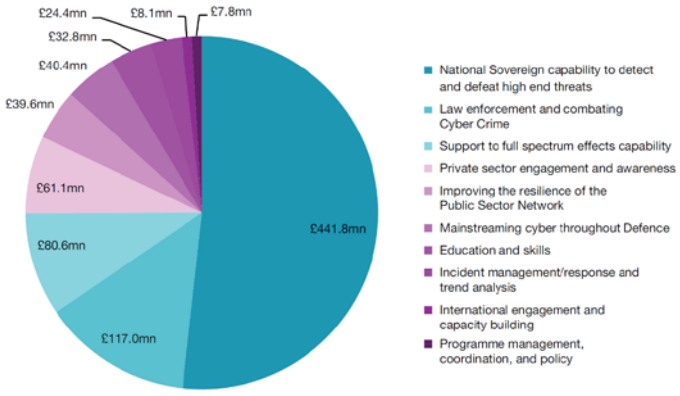
A efectos de desarrollar las actividades necesarias de respuesta a ciberincidentes, el Gobierno Federal se guiará por los siguientes principios:

- Responsabilidad compartida.
- Respuesta basada en el riesgo.
- Respetar a las entidades afectadas.
- Unidad de esfuerzo gubernamental.
- Facilitar la recuperación.

Terminando con las actividades de los Estados Unidos, en diciembre de 2016 la Commission On Enhancing National Cybersecurity publicó el ***Report on Securing and Growing the Digital Economy*****,** que desarrolla las siguientes acciones:

- Proteger, defender y asegurar la actual infraestructura de la información y las redes digitales.
- Innovar y acelerar la inversión para la seguridad y el crecimiento de las redes digitales y la economía digital.
- Preparar a los consumidores a prosperar en una era digital.
- Generar perfiles con capacidades técnicas para desarrollar la ciberseguridad.
- Mejorar los sistemas gubernamentales para que funcione de manera efectiva y segura.
- Garantizar una Economía Digital Global Abierta, justa, competitiva y segura.

Entre 2011 y 2016, el gobierno del **Reino Unido** financió un Programa Nacional de Ciberseguridad con un presupuesto de 860 millones de libras para ejecutar la Estrategia Nacional de Ciberseguridad de 2011-2016. Por su interés reproducimos el desglose de las partidas a las que se asignaron dichos fondos[208].



208 Fuente: UK Cabinet Office: The UK Cyber Security Strategy 2011-2016. Annual Report. April 2016

Además, en 2016, el **Reino Unido** publicó su ***National Cyber Security Strategy 2016-2021***, actualizando la previa de 2011. La nueva estrategia e fundamenta en los siguientes pilares a las que se asocian diferentes medidas: Defensa, Disuasión, Desarrollo, Acción Internacional y Métricas.

En junio de 2016, la **Unión Europea** publicó su ***A Global Strategy for the European Union's Foreign And Security Policy*****,** en la que se incluyen acciones en materia de ciberseguridad. En este documento se señala que la UE centrará su atención también en la ciberseguridad ayudando a los Estados miembros a protegerse contra las ciberamenazas, manteniendo al tiempo un ciberespacio abierto, libre y seguro, lo que implica el fortalecimiento de las capacidades tecnológicas encaminadas a mitigar las amenazas y la resiliencia de las infraestructuras, redes y servicios críticos y reducir el ciberdelito. Este compromiso señala la necesidad de fomentar sistemas TIC innovadores que, asegurando la disponibilidad e integridad de los datos, garantice al mismo tiempo la seguridad en el espacio digital europeo mediante políticas adecuadas sobre la ubicación del almacenamiento de datos y la certificación de productos y servicios digitales. El documento requiere, además, considerar las cuestiones de ciberseguridad en todas las áreas políticas, reforzar los elementos *ciber* en las misiones y operaciones de la PCSD y desarrollar más las plataformas de cooperación.

Es deseo de la UE apoyar la cooperación política, operacional y técnica entre los Estados miembros, en particular en materia de análisis e impacto de los ciberataques, y fomentará las evaluaciones compartidas entre las estructuras de la UE y las instituciones pertinentes de los Estados miembros. Asimismo, aumentará su cooperación en ciberseguridad con socios fundamentales como los Estados Unidos y la OTAN. La respuesta de la UE también estará integrada en sólidas asociaciones público-privadas. La cooperación y el intercambio de información entre los Estados Miembros, las instituciones, el sector privado y la sociedad civil pueden fomentar una cultura común de seguridad cibernética y aumentar la preparación para responder a ataques.

La **Organización para la Seguridad y la Cooperación en Europa (OSCE),** en diciembre de 2016, publicó la Decisión nº 5/16, ***Esfuerzos de la OSCE para reducir los riesgos de conflicto dimanantes del uso de las tecnologías de la información y las comunicaciones****,* que, respaldando la adopción de la Decisión Nº 1202 del Consejo Permanente, de 10 de marzo de 2016, relativa a las medidas de fomento de la confianza de la OSCE para reducir los riesgos de conflicto dimanantes del uso de las tecnologías de la información y las comunicaciones, y de que se elaboren nuevas medidas de fomento de la confianza que sean conformes a las consideraciones enunciadas en la Decisión Nº 1202 del Consejo Permanente, y alienta a todos los Estados participantes a que contribuyan a la aplicación de estas medidas.

La **Unión Internacional de Telecomunicaciones** (ITU) publicó el ***Índice Mundial de Ciberseguridad,*** a partir de la iniciativa ***Global Cybersecurity Agenda***, un marco de trabajo para la cooperación internacional que busca aumentar la confianza y seguridad en la sociedad de la información. La CGA tiene como base cinco pilares estratégicos o áreas de trabajo:

- Medidas legales,

- Medidas técnicas y de procedimiento,
- Estructuras organizacionales,
- Creación de capacidad,
- Cooperación internacional.

A partir de ellas surge el Índice Mundial de Ciberseguridad (*Global Cybersecurity Index*), que tiene como objetivo medir y evaluar el compromiso de los países en la materia. Desarrollado inicialmente en 2013, el GCI se encuentra en un proceso de actualización constante para determinar aspectos relevantes de la seguridad de los países miembros de la ITU. El índice tiene como propósito medir los siguientes elementos:

- Tipo, nivel y evolución del compromiso con la ciberseguridad en los países a través del tiempo.
- Avances en el compromiso con la ciberseguridad de todos los países.
- Avances en el compromiso con la ciberseguridad desde una perspectiva regional.
- Nivel de participación de los países en las iniciativas de ciberseguridad.

El GCI pretende ser un punto de referencia para que los países puedan identificar áreas de oportunidad en el campo de la ciberseguridad. Al mismo tiempo, puede funcionar como un incentivo para que los estados naciones busquen mejorar su clasificación o su evaluación relativa al GCI, lo que, sin duda, permite elevar su nivel de ciberseguridad. El Índice funciona a partir de un cuestionario que considera 24 indicadores. El documento se divide en cinco secciones: la primera de ellas considera las legislaciones o reglamentos sobre ciberseguridad en el país en cuestión, por ejemplo, si se cuenta con leyes relacionadas a accesos no autorizados, el uso indebido de sistemas de información o la intercepción de datos.

Algunas iniciativas internacionales específicas

La **utilización de software comercial** ha sido puesta últimamente en entredicho por distintos actores nacionales. Alegando, en muchas ocasiones, motivos de seguridad y de Defensa. Esto ha conducido a la aparición de varias iniciativas internacionales que pretender obviar el uso de software comercial, potenciando el uso software específico, basado en muchas ocasiones en software libre. Seguidamente se resumen las más significativas de tales iniciativas[209].

Con la llegada de Windows 8 y el fin del soporte del sistema operativo Windows XP el gobierno de **China** vetó la instalación del sistema operativo Windows en los sistemas gubernamentales[210]. Hasta entonces, China se encontraba dentro del programa por el que se proporciona a gobiernos y otras organizaciones acceso al código fuente del sistema operativo y de las principales herramientas de la empresa. De esta forma, es posible analizar el código para diagnosticar la existencia de errores de diseño o de programación y para comprobar que no existen puertas traseras que permitan el acceso a terceras personas. Al no poder acceder al código fuente consideró que utilizar ese

209 Fuente directa: IEEE. David Ramírez Morán: Confianza y estrategia en las tecnologías de la información. (2016)

210 Fuente: Reuters: "China bans use of Microsoft's Windows 8 on government computers" (véase: http://www.reuters.com/article/us-microsoft-china-idUSBREA4J07Q20140520)

sistema operativo, así como las aplicaciones ofimáticas suponía un riesgo para su información. Por otro lado, en lo que respecta al hardware, China se encuentra en proceso de fabricación propio para hacer frente a la limitación impuesta por Estados Unidos a la exportación de coprocesadores utilizados en sistemas informáticos de procesado de altas prestaciones. En 2002 se creó en China la iniciativa de colaboración público privada denominada BLX para la creación de los microprocesadores denominados inicialmente Godson y actualmente Loongson[211], así como las herramientas necesarias para el desarrollo y diseño de sistemas con estos procesadores.

En **Rusia**, la eliminación del sistema operativo Windows se debe a una política puesta en marcha por Vladimir Putin en 2010 por la que planteaba 2016 como fecha límite para eliminar los equipos cuyo sistema operativo fuera Windows de las administraciones públicas y sustituirlo por software de fuentes abiertas[212]. El Gobierno ruso afirma que el motivo de desarrollar equipamiento informático propio es el de "sustituir los modelos extranjeros que no garantizan la ausencia de spyware o protección contra las fugas de información"[213]. Para ello, en 2014 creó *United Instrument Manufacturing Corporation* (UIMC), una filial de la empresa rusa estatal Rostec, en la que se agrupan instalaciones de investigación y producción del sector de la radio y la electrónica[214].

Recientemente, publicaba UIMC la noticia de que pasará a producción la última versión de su microprocesador Elbrus-8C, que cuenta con 8 núcleos. Se trata de un dispositivo con arquitectura SPARC que, al igual que el dispositivo desarrollado por China, incorpora traductores binarios que permiten la ejecución de instrucciones de las arquitecturas x86, así como de las arquitecturas ARM diseñadas por la empresa inglesa. Al igual que en el caso de China, el desarrollo de un sistema operativo basado en Linux da esa doble respuesta al problema de permitir contar con un sistema operativo eficiente y que permite explotar al máximo las prestaciones de sus dispositivos por utilizar una arquitectura SPARC, que también se encuentra entre las soportadas por Linux.

Corea del Norte es otro de los países que ha tenido que tomar una iniciativa para contar con tecnologías de la información que le permitan aprovechar las ventajas asociadas. En su caso, se ha optado también por desarrollar un sistema operativo propio basado en Linux, denominado Red Star y del que se han filtrado recientemente informaciones sobre la publicación de la versión 3[215].

En **India** también se está introduciendo una solución de software libre basada en Linux con el sistema operativo Bahrat Operating System Solutions (BOSS)[216], que ya va por su versión 5 desde que fuera lanzado en 2007, y con el que se prevé sustituir el sistema operativo Windows de los ordenadores gubernamentales.

211 Véase: http://www.loongson.cn/index_en.html

212 Fuente: Computer World: «Putin to put Russian government on Linux by 2015» (véase: http://www.computerworld.com/article/2511966/government-it/putin-to-put-russian-government-on-linux-by-2015.html)

213 Véase: http://www.eng.opkrt.ru/index.php/news/205-uimc-started-developing-equipment-based-on-russian-processor-and-protected-from-cyberespionage

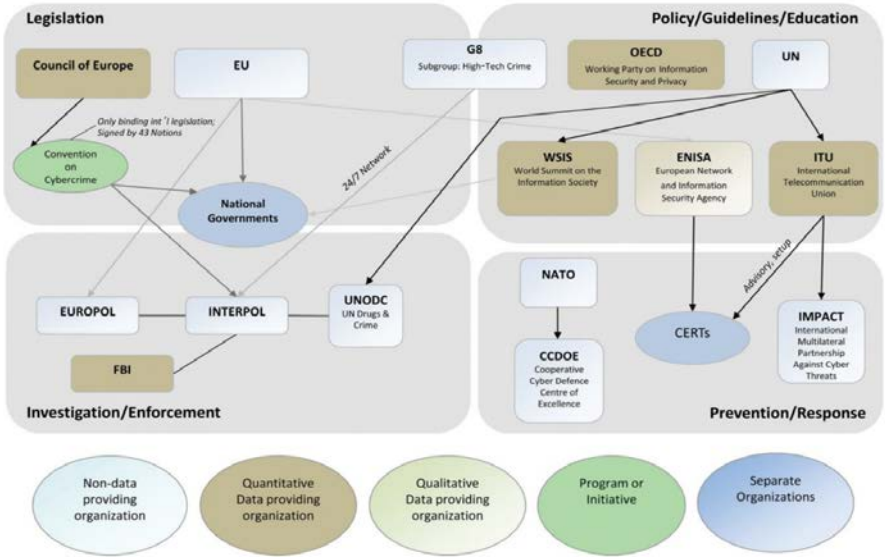
214 Véase: http://www.eng.opkrt.ru/index.php/corporation/about-the-corporation

215 Véase: http://www.theguardian.com/world/2015/dec/27/north-koreas-computer-operating-system-revealed-by-researchers

216 Véase: http://trak.in/tags/business/2015/09/15/boss-os-made-in-india-operating-system-boss-replace-microsoft-windows/

Varios países de Europa se han embarcado también en la sustitución de productos comerciales por herramientas de software libre con funcionalidades similares o equivalentes. Por ejemplo, el Ministerio de Interior de **Francia** ha sustituido las herramientas ofimáticas de Microsoft por herramientas de software libre[217], al igual que está haciendo el gobierno de **Italia**[218], que por una ley promulgada en 2012 debe migrar los sistemas gubernamentales a herramientas de software libre, o **Polonia** con las herramientas de correo electrónico[219]. Los **Países Bajos** es otro de los países en los que el software libre también se está utilizando en el Ministerio de Defensa[220].

Finalmente, es necesario remarcar que la complejidad en el tratamiento de las ciberamenazas también pasa por considerar el importante volumen de actores implicados en su tratamiento. La figura siguiente muestra un esquema global con los actores más significativos y sus interdependencias[221].



8.5 Iniciativas nacionales: el Esquema Nacional de Seguridad.

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

En noviembre de 2016 entraron en vigor 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. Ambas constituyen el eje vertebrador de las relaciones de los ciudadanos y sus Administraciones Públicas y de estas entre sí, consagrándose el uso de las herramientas electrónicas como el medio habitual para encauzar tales relaciones.

217 Véase: https://joinup.ec.europa.eu/community/osor/news/frances-defence-ministry-dutiful-studies-free-software

218 Véase: https://joinup.ec.europa.eu/community/osor/news/italian-military-switch-libreoffice-and-odf

219 Véase: https://joinup.ec.europa.eu/community/osor/news/frances-defence-ministry-dutiful-studies-free-software

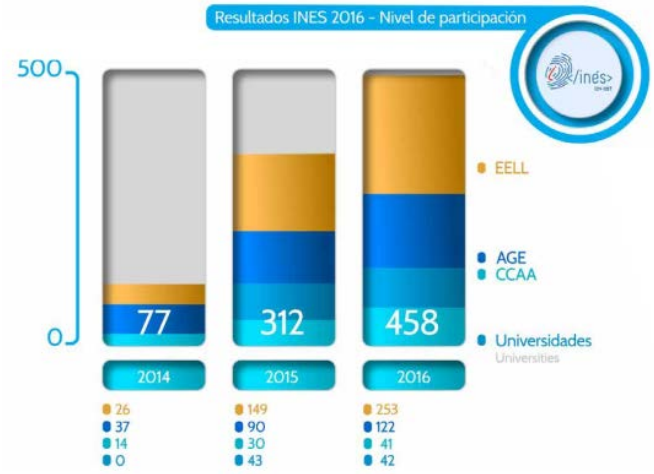
220 Véase: https://joinup.ec.europa.eu/community/osor/news/open-source-advancing-dutch-defence-ministry

221 Fuente: Nazli Choucri, Stuart Madnick y Priscilla Koepke: Institutions for Cyber Security: International Responses and Data Sharing Initiatives - Working Paper CISL# 2016-10 (August 2016).

La necesidad de articular elementos de protección a la antedicha universalización de la relación electrónica, unido al incremento en el ámbito subjetivo de aplicación de las antedichas normas, han hecho especialmente importante la observancia escrupulosa del **Esquema Nacional de Seguridad (ENS)**, regulado en el RD 3/2010, de 8 de enero y actualizado por RD 951/2015, de 23 de octubre, como elemento normativo capaz de garantizar la adecuada protección de la información tratada y los servicios prestados por las entidades del sector público.

Para ello, tal y como dispone el propio ENS, en 2016 se publicaron dos Instrucciones Técnicas de Seguridad[222]:

1) Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la **Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad**. En ella se establecen las condiciones relativas a la recopilación y comunicación de datos que permita conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito del ENS, y confeccionar un perfil general del estado de la ciberseguridad en las Administraciones públicas. Para este fin, el Centro Criptológico Nacional (CCN) ha desarrollado la herramienta **INES**[223] (Informe Nacional del Estado de Seguridad) que cuenta con una plataforma telemática, a través de la cual los organismos pueden tener un conocimiento más rápido e intuitivo de su nivel de adecuación al ENS y del estado de seguridad de sus sistemas. Hasta la fecha, el CCN ha elaborado tres Informes en función de los datos recogidos en INES, alcanzando una participación de 458 organismos en 2016 (frente a los 77 de 2014, lo que representa un incremento del 495%), procedentes de la Administración General del Estado, Comunidades Autónomas, Entidades Locales y Universidades (invitadas a través de la Conferencia de Rectores de Universidades Españolas, CRUE).



222 (Ambas en BOE Núm. 265, miércoles 2 de noviembre de 2016)

223 https://www.ccn-cert.cni.es/ens/ines.html

1) Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la **Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad**. Tiene por objeto establecer los procedimientos para dar publicidad a la conformidad con el Esquema, así como los requisitos exigibles a las entidades que quieran certificar el cumplimiento con el ENS

Ambas normas, de obligado cumplimiento para los sistemas de información concernidos del ámbito subjetivo de aplicación del ENS, organizan el modo común de actuar de las entidades públicas en la garantía de la eficacia de las medidas de seguridad y el conocimiento global del estado de la seguridad pública.

9. TENDENCIAS PARA 2017

Según los datos examinados y las fuentes consultadas, parece claro que las amenazas en 2017 serán más sofisticadas y dirigidas. Los siguientes párrafos muestran las tendencias más probables para este año[224].

1. **Respuesta institucional al ciberespionaje:** Los estados atacantes han perseguido datos de naturaleza política o económica de las entidades atacadas. Las entidades-víctima se localizaron en el sector gubernamental o, en algunos casos, en individuos o miembros de un partido político. El modus operandi de todos estos ataques es similar y es presumible que no cambie significativamente en 2017. Las diferentes fases de ataque no cambiarán significativamente, pero las vulnerabilidades y técnicas se han vuelto mucho más difíciles de detectar. Por todo ello, es de esperar que el ciberespionaje se mantenga muy activo en 2017, ya sea como parte de las operaciones de inteligencia de un estado-nación o dirigido por grupos organizados que proporcionarán servicios de ataque o buscarán información de interés y la podrán a la venta.

   Finalmente, la fuga de información sobre capacidades de grupos (Snowden y Vault 7) evidencia que existen procedimientos de ataque sobre los que la defensa es muy difícil. Se deben articular mecanismos de intercambio de información más ágiles en 2017 para poder responder a esta amenaza.

2. **Redefinición de las inversiones en TIC:** Atendiendo a una encuesta internacional de SalesForce, el 68% de los equipos informáticos manifiestan que invertirán más en aplicaciones móviles, migración a la nube y ciberseguridad / respuesta a incidentes en los próximos ejercicios[225]. Al mismo tiempo, el 63% planea aumentar el gasto en aplicaciones orientadas al cliente como se muestra en la figura siguiente. Obsérvese que la ciberseguridad aparece en los primeros lugares, equiparada a las inversiones en aplicaciones móviles o migración a la nube.

224 Datos de elaboración propia y recabados de las siguientes fuentes: Kaspersky Lab: Predictions for 2017: 'Indicators Of compromiso Are Dead' y McAfee Labs: 2017 Threats Predictions. November 2016

225 Fuente: SalesForce Research: 2016 State Of IT.

3. **Surgimiento de nuevos tipos de ataques complejos**: Todo parece indicar que los tradicionales Indicadores de Compromiso pueden no ser tan efectivos cuando se emplean las propias capacidades del Sistema Operativo. Ataques que se denominan "sin malware".

   En los últimos años, el número de incidentes relacionados con APT ha crecido significativamente. Sin embargo, pocos de los actores de la amenaza descritos habitualmente en los medios de comunicación son realmente "avanzados".

   Estas son algunos de los elementos que caracterizan a los grupos de ciberespionaje más "avanzados":

   - Uso de exploits de día-cero.
   - 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.
   - Soportar múltiples canales de exfiltración.
   - Código dañino en memoria de los equipos, sin utilizar el disco.
   - Técnicas de persistencia avanzadas que utilizan funciones no documentadas.

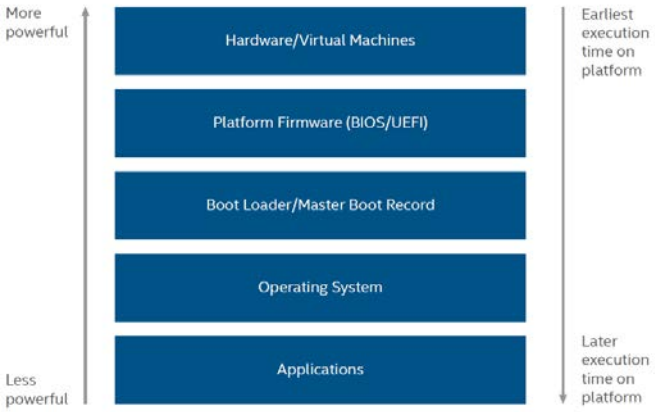
   Todo ello hace que sea necesario incrementar y ampliar las capacidades de vigilancia basadas en anomalías y mejorar el intercambio de patrones de detección en cualquier formato (IOC, reglas Yara, etc.).

4. **Infecciones efímeras:** La adopción de PowerShell, al mismo tiempo que constituyó un importantísimo avance para los administradores de sistemas Windows[226], es también una importante herramienta que pueden usar los agentes de las amenazas para el desarrollo de nuevos tipos de código dañino que persigan un despliegue aún más sigiloso, y que posibilite movimientos laterales y capacidades de reconocimiento que probablemente no se obtendrían en configuraciones estándar. Esto podría dar al atacante un tiempo limitado (pero muy valioso) para obtener la información perseguida. Por este motivo, para 2017 se incrementará el descubrimiento de estas "infecciones efímeras", tales como código dañino residente en memoria y destinado a

226 Windows Powershell es un programa basado en línea de comandos de ayuda a los administradores de una red a lograr una mejor y más rápida administración e implementación en su entorno. Hace uso de comandos interactivos y comandos base denominados "cmdlets" (commandlets), permitiendo una mayor eficiencia y menor trabajo por parte de los profesionales o administradores de sistemas. Powershell amplía las capacidades y características de "cmd" y, además, incorpora la posibilidad de escribir y ejecutar scripts de forma nativa y automatizar tareas fácilmente.

reconocimiento general y recolección de credenciales, **sin interés por persistir en el sistema de la víctima**. Este tipo de mecanismo permitirá operar a los atacantes hasta que un reinicio limpie su infección de la memoria, Esta nueva situación exige el concurso de nuevas y más sofisticadas herramientas de detección.

5. **Amenazas al hardware y firmware:** Este tipo de amenazas constituirán en 2017 un objetivo creciente para los atacantes más sofisticados. El software, incluidos los sistemas operativos y las aplicaciones, dependen implícitamente del hardware para funcionar correctamente. Las vulnerabilidades de hardware pueden socavar el funcionamiento y la seguridad de toda la pila de software. La explotación de una vulnerabilidad de hardware puede comprometer todo un sistema y no requiere una explotación completa de la pila de software (ver figura). Además, los sistemas cuyo hardware es atacado con éxito pueden ser difíciles de reparar sin reemplazar el hardware vulnerable. Finalmente, no se puede confiar en ninguno de los mecanismos y protecciones de seguridad basados en software de los sistemas porque asuman que el hardware no ha sido comprometido.



6. **Dispositivos móviles como objetivo de acciones de ciberespionaje:** Durante los últimos años se ha detectado una multiplicidad de código dañino dirigido a dispositivos móviles227, aunque la mayor parte de las campañas en las que se utilizaron se basaban en kits de herramientas para ordenadores de escritorio. Sin embargo, como cada vez es más frecuente el uso de dispositivos móviles en ambientes profesionales, se espera que durante 2017 se incrementen las campañas de ciberespionaje dirigidas a dispositivos móviles.

   Es esperable el crecimiento del código dañino para dispositivos móviles en 2017, destacando el ransomware, troyanos bancarios y herramientas de acceso remoto. Puesto que los dispositivos móviles suelen estar respaldados en la nube, el éxito de los pagos directos de rescate para desbloquear dispositivos suele ser limitado. Debido a eso, los autores de malware móvil combinarán bloqueos de dispositivos móviles con otras formas de ataque, como el robo de credenciales. Es previsible que en 2017 los troyanos bancarios reaparezcan de la mano de autores de ransomware. Este malware

227 Tales como Sofacy, RedOctober, CloudAtlas, así como clientes de HackingTeam y la sospechosa suite NSO Pegasus para iOS.

combinará bloqueos de dispositivos móviles y otras características de ransomware con los ataques tradicionales de "man in the middle" para sustraer factores de autenticación primarios y secundarios, permitiendo a los atacantes acceder a cuentas bancarias y a tarjetas de crédito.

7. **Ataques a entidades financieras:** Los ataques contra la red SWIFT de 2016 han vuelto a poner el foco de los agentes de las amenazas en las entidades financieras -más que en sus usuarios- como víctimas finales de sus acciones[228]. A medida que crezca el interés de los ciberdelincuentes, es de esperar ver el aumento de mecanismos de tipo SWIFT en el desarrollo de acciones delictivas por parte de grupos consolidados. Realizar una de tales acciones requiere acceso inicial, software especializado, paciencia y, eventualmente, un plan de blanqueo de dinero. Cada una de estas acciones exige la presencia de un delincuente especializado, capaz de proporcionar sus servicios a un precio determinado. Lo único novedoso será la pieza de software requerida para el desarrollo de tal tipo de ataques. Por tanto, no será raro presenciar en 2017 la comercialización de este tipo de ataques a través de recursos especializados que se ofrecen a la venta en foros underground o mediante servicios del tipo Crime-as-a-service.

   Finalmente, a la vista de que las últimas implementaciones de seguridad de los medios de pago de los clientes finales han dado sus frutos, es probable que 2017 sea testigo de un incremento de los ataques directamente contra las infraestructuras tecnológicas del sistema de pagos.

8. **Relación de confianza derivada de un ataque por ransomware**: Curiosamente, el ecosistema criminal del ransomware puede tener lugar en base al principio de que el atacante respetará un contrato tácito con la víctima por el que, una vez reciba el pago, se devolverán los archivos bloqueados. Durante los últimos años, los ciberdelincuentes han exhibido una sorprendente apariencia de profesionalismo en el cumplimiento de aquella promesa, permitiendo que el modelo delincuencial prospere. Sin embargo, puesto que la popularidad del ransomware sigue en aumento, es muy posible que aparezcan atacantes que no cumplan la promesa y desbloquear los ficheros bloqueados. Con ello se puede provocar una crisis de confianza que conduzca a pensar que "pagar el rescate" no conduce a nada.

   Sea como fuere, el ransomware seguirá siendo una amenaza muy significativa en 2017. El Ransomware-as-a-Service, personalizado para la venta como servicio, y los derivados de código abierto mantendrán ocupada a la industria de seguridad, pese al impacto que podrían tener iniciativas tales como "No More Ransom!"[229].

9. **Ciberataques contra Sistemas de Control Industrial:** Aunque sabemos que, en la actualidad, un accidente industrial inducido por un cibersabotaje no es algo excesivamente probable[230], mientras que las Infraestructuras Críticas y los sistemas de

228 El ataque Carbanak, descrito en varios informes del CCN, ha sido el más significativo ataque contra entidades financieras, usando los métodos, procedimientos y herramientas tradicionalmente usados por las APT.

229 Véase: https://www.nomoreransom.org/

230 Pese al ejemplo de Stuxnet.

fabricación continúen conectados a Internet, a menudo con poca o ninguna protección, estos objetivos siguen estimulando el apetito de los atacantes. Es importante tener en cuenta que, además del alarmismo, estos ataques requieren ciertas habilidades y determinadas intenciones pues no persiguen beneficio económico.

10. **Cooperación entre las industrias de la 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 más integrales. Los proveedores de soluciones de ciberseguridad comenzarán a prestar servicio y dar soporte a los proveedores de seguridad física ofreciendo nuevo software, plataformas y arquitecturas para la integración.

11. **Débil seguridad del Internet de las Cosas (IoT)**: Como la botnet Mirai demostró en 2016, la débil seguridad de cierto tipo de dispositivos conectados a Internet proporciona una oportunidad para los atacantes para causar el caos con poca o ninguna responsabilidad. La figura siguiente muestra el impacto económico de la IoT en los próximos años[231].

A medida que los fabricantes de dispositivos IoT sigan produciendo dispositivos no seguros, que causen problemas a gran escala, es probable que determinado tipo de atacantes" asuman la "responsabilidad" de "parchear" los sistemas vulnerables. En el peor de los casos, esta situación podría dar como resultado la necesidad de desactivar por completo los dispositivos vulnerables.

Además, hay que tener en cuenta que, en lugar de atacar a un fabricante específico e intentar alterar su código base, es más fácil crear una versión "gratuita" de una biblioteca de código ampliamente utilizada, que contenga una puerta trasera y ofrecerla a muchos fabricantes de dispositivos IoT. En 2016 se ha observado código dañino en bibliotecas de código ampliamente utilizadas en Android. Por tanto, en los próximos 12 a 18 meses, veremos código dañino ocultándose en bibliotecas ampliamente utilizadas o incrustado directamente en los dispositivos utilizados en el espacio IoT del consumidor.

231 Fuente: McKinsey Global Institute.

12. **Dronejacking**, aparece cada vez con más frecuencia en la lista de objetivos de las amenazas. Los drones están en camino de convertirse en una herramienta importante para las entidades de mensajería, las agencias policiales, los fotógrafos, los agricultores, los medios de comunicación, etc. Es difícil negar que los drones se han vuelto mucho más valiosos para muchos tipos de negocios y agencias gubernamentales. Se han visto ejemplos de ataque empleando un drone equipado con una completa suite de hacking que le permitiría aterrizar en el techo de un edificio para tratar de penetrar en la red inalámbrica local.

13. **Revelación descontrolada de vulnerabilidades**: Como era de esperar, a la publicación del paquete ShadowBrokers, que incluía una gran cantidad de exploits para múltiples firewalls de distintos fabricantes, siguió la evidencia de múltiples ataques contra tales equipamientos, que los fabricantes pretendieron atajar con la publicación de los correspondientes parches. Sin embargo, la magnitud de las consecuencias aún no se ha tenido en cuenta totalmente: ¿Qué tipo de implantes dañinos pueden estar actualmente inactivos en tales dispositivos vulnerables? He aquí la paradoja subyacente: dispositivos creados para impedir la entrada de atacante, que posibilitan su penetración. No es descabellado pensar, por tanto, que 2017 traiga noticias de nuevos ataques contra este tipo de dispositivos.

14. **Guerra de la información…. y la desinformación**: Con la creación de falsos puntos de venta -que facilitaban descargas dañinas o posibilitaban acciones de extorsión-[232] de éxito reconocido, es de esperar que esta llamada "guerra de información… y de desinformación" continúe en 2017, manipulando la información y la generación de una opinión pública errónea. El verdadero peligro en ese momento es que a medida que los periodistas y los ciudadanos se acostumbran a aceptar como verdaderos datos torticeramente obtenidos, están abriendo la puerta a más actores interesados en la manipulación de la información.

15. **Disuasión y la atribución de la autoría:** A medida que los ciberataques lleguen a desempeñar un papel más importante en las relaciones internacionales, la atribución se convertirá en un tema central en la determinación de las propuestas geopolíticas. No están definidos las evidencias necesarias para acusar formalmente -y ante la opinión pública- a un atacante de una determinada acción. Como quiera que la atribución exacta es casi imposible, esta realidad puede conducir a que un "señalamiento libre" se considere suficientemente bueno para atribuir un hecho a un determinado autor. Aunque es sabido que siempre debe actuarse con enorme cautela, no es menos cierto que existe una necesidad real de que los ataques tengan consecuencias. Una de las preocupaciones más extendidas en la actualidad, es asegurar que las represalias no generan una escalada y se puedan detectar las banderas falsas. Por ello se incrementará el uso de software dañino comercial[233].

16. **Deseo de anonimato:** Constituye un lugar común señalar el valor de eliminar los vestigios de anonimato que permanecen en el ciberespacio, en beneficio de

232 Tales como Lazarus o Sofacy.

233 Tales como las herramientas Cobalt Strike y Metasploit.

anunciantes... o espías. Para los primeros, el seguimiento con cookies persistentes ha demostrado ser una técnica valiosa. Es probable que en 2017 esta realidad se amplíe aún más y se combine con widgets y otras adiciones inocuas a sitios web, que permitan a las compañías rastrear los hábitos de navegación de los usuarios. Por otro lado, activistas y Ciberyihadistas usarán técnicas de anonimización para evitar su localización en redes sociales.

17. **Publicidad como herramienta de ataque**: Como hemos señalado en este Informe, ninguna tecnología actual es más capaz de permitir ataques dirigidos que las redes publicitarias. Su ubicación ya está totalmente motivada, desde el punto de vista económico, y hay poca o ninguna regulación, como lo demuestran los recurrentes ataques por malvertising en los principales sitios web. Por su propia naturaleza, las redes publicitarias proporcionan perfiles de usuarios excelentes (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.

18. **Disminución de las vulnerabilidades en Windows**: La explotación de vulnerabilidades de software del lado del usuario se ha vuelto mucho más difícil en los últimos años, aumentando el coste del desarrollo de exploits fiables. Para penetrar con éxito en los últimos sistemas (por ejemplo, un navegador Microsoft Edge bajo sistema operativo Windows de 64 bits), los atacantes deben combinar varias vulnerabilidades con técnicas avanzadas de explotación[234].

19. **Vulnerabilidades en tecnologías**: Se estima que el coste de vulnerabilidades día 0 de las tecnologías Apple y Microsoft se incrementará considerablemente. Se espera durante 2017 una reutilización de las vulnerabilidades y herramientas publicadas en Wikileaks. Los fabricantes deberán forzar el calendario de actualizaciones para mitigar esta amenaza. Además, se resalta la evolución en las siguientes tecnologías:

    Adobe Flash: Seguirá siendo el objetivo principal de los ataques basados en vulnerabilidades. Las vulnerabilidades de día-cero, como CVE-2016-4117 y CVE-2016-1019, representaron alrededor del 50% de todos los ataques de día cero descubiertos por las compañías de seguridad en 2016.

    Microsoft Internet Explorer y Edge: Los ataques dirigidos a IE y Edge continúan siendo mínimos. En 2016 no se ha observado un auténtico exploit de día cero para estas plataformas[235].

    Java, PDF y Microsoft Office: Durante 2016 se ha informado de numerosos ataques a aplicaciones Java, PDF y Office. En 2017 se espera que se sigan utilizando para infecciones relacionadas con Ciberespionaje y cibercrimen.

    Windows kernel: Aunque se han implementado algunos mecanismos de seguridad (protección de ejecución en modo supervisor, filtrado de llamadas del sistema Win32, mejoras en la asignación del espacio de direcciones del núcleo, etc.), la existencia de explotaciones en modo kernel continúa siendo significativa.

    Software de Infraestructura de comunicaciones: Es previsible que los ataques contra las

234 Como lo demuestran los concursos de hacking, tales como Pwn2Own, 2016.

235 Aunque los exploits CVE-2016-0189 y CVE-2016-0034 se entregan y ejecutan desde un navegador, en realidad son vulnerabilidades del motor de secuencias de comandos y de .NET, respectivamente.

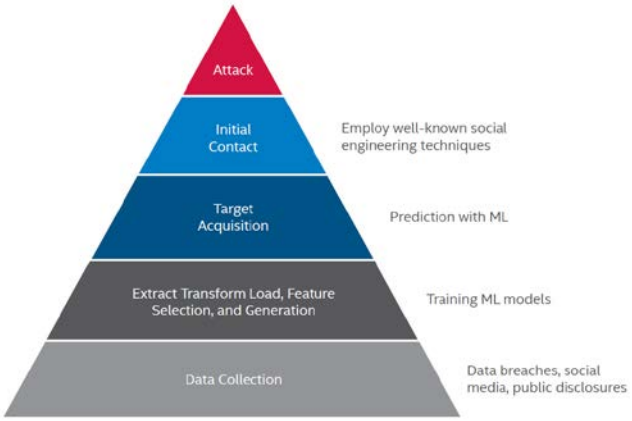
vulnerabilidades de la infraestructura de comunicaciones serán muy activos en 2017. Atendiendo a la lista de OpenSSL, se observan muchas vulnerabilidades parcheadas en cada versión. Además de OpenSSL, también encontramos vulnerabilidades críticas en otro software de código abierto para la resolución de nombres de dominio[236].

Componentes *Legacy* frente a nuevas características: Aunque la mayoría de los autores de código dañino se centran en nuevas características, como el subsistema de Windows para Linux, otros se han centrado en componentes *legacy*. Desde que se descubrió la vulnerabilidad crítica *GHOST* (CVE-2015-0234), y que vino existiendo desde hace 15 años, los investigadores de seguridad han comenzado a reexaminar el código *legacy*.

Software de virtualización: Con la continua adopción de la tecnología tanto en la nube como en los sistemas de las organizaciones, la seguridad de la virtualización es un tema candente que ha atraído la atención de investigadores de seguridad… y de los atacantes. Se estima que se incremente el desarrollo de nuevos ataques en 2017.

Productos de seguridad: En 2016, se han observado muchas vulnerabilidades graves en productos de seguridad. A principios de año, los investigadores de Google encontraron una grave vulnerabilidad de ejecución remota de código en los dispositivos FireEye y en la mayoría de los principales proveedores de antimalware. En el verano, los datos filtrados de *Equation Group* revelaron muchas vulnerabilidades (incluyendo algunas de día cero) dirigidas a varios productos cortafuegos. Esta tendencia continuará sin duda en 2017.

20. **Aprendizaje automático (machine learning) como catalizador 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). En 2016 hemos visto a entusiastas y científicos enseñar a las máquinas cómo escribir sonetos shakesperianos, componer música, pintar como Picasso y derrotar a jugadores profesionales. El período de aprendizaje se ha reducido y la accesibilidad para todos -incluidos los cibercriminales- nunca ha sido mejor. La ciberseguridad es una carrera en la que el aprendizaje automático está colaborando en nuevas técnicas cada vez más efectivos[237].



21. **Ataque a la privacidad como herramienta del ciberactivismo:** Con los años, el volumen recabado de datos sobre los usuarios ha aumentado exponencialmente, haciendo que la información agregada ha tenido múltiples aplicaciones

236 CVE-2015-7547 (un desbordamiento de búfer en el cliente de DNS) y CVE-2016-5696 (una brecha de Linux que permite el secuestro del tráfico de Internet).

237 Fuente: McAfee Threats Predictios 2017.

beneficiosas[238]. En 2016 siguió en aumento la concienciación sobre la información obtenida de los dispositivos de los usuarios y el tamaño de la llamada “huella digital”, y seguirá aumentando en 2017. Teniendo en cuenta estas tendencias, podemos predecir que en 2017 los hacktivistas usarán esta oportunidad para "educar a los usuarios" sobre el volumen de datos que los propios usuarios están filtrando al exterior, mediante ataques que recopilan datos (búsquedas, enlaces, conexiones, vistas de páginas, uso de productos, etc.) para, a continuación, exhibir tales contenidos públicamente.

22. **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 las amenazas. Este cambio de tendencia pudo observarse en 2016[239]. En 2017, la CTA continuará colaborando en mejorar la defensa colectiva, con nuevas investigaciones para responder adecuadamente a nuevos ataques.

238 La utilidad práctica de la agregación de datos se menciona, incluso, en la Guía de la Comisión Europea sobre el Privacy Shield entre la UE y los EE.UU.

239 Miembros fundadores de la Cyber Threat Alliance (CTA) colaboraron en la investigación de la campaña CryptoWall Versión 3. Poco después de publicar el resultado de sus investigaciones, los autores de este código dañino abandonaron su enfoque anterior, para concentrarse en una nueva campaña: la versión 4. Véase: http://cyberthreatalliance.org/members.html