Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación
Retrospectiva sobre la Seguridad de la Información en 2016

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-10062-170118*
Edición:	*1*
Categoría	*Público*
Fecha de elaboración:	*17/01/2017*
N° de Páginas	*1 de 36*

1 Tabla DE CONTENIDOS

2 OBJETO

El objeto de este documento es realizar un pequeño resumen de los aspectos más relevantes acaecidos en el año 2016 en relación a la seguridad de la información.

3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Es de carácter informativo y pretende realizar una retrospectiva de los sucesos más importantes que han tenido lugar a lo largo del año 2016 relativos a la seguridad de la información a nivel global. De esta forma el lector podrá tener una visión de conjunto de los aspectos más relevantes sobre la ciberseguridad del pasado año 2016.

4 INTRODUCCIÓN

Hace apenas unos días que hemos despedido al 2016 y le hemos dado la bienvenida a un nuevo año que vendrá cargado de novedades. No obstante, los ecos de lo acontecido durante el año recién finalizado aún perduran.

Desde AndalucíaCERT hemos considerado oportuno realizar un informe en el que se destaquen los hitos más importantes que han tenido lugar durante el pasado año, ya que 2016 ha demostrado, una vez más, la importancia de la seguridad de la información.

A las ya tradicionales fugas de información que se producen periódicamente en todo tipo de organizaciones, el interminable listado de nuevas vulnerabilidades descubiertas y las clásicas acciones delictivas perpetradas por grupos de cibercriminales (SPAM, phishing, botnets, ataques DDoS...), hay que sumar el afianzamiento de nuevos modelos de fraude online como el ransomware, el aprovechamiento de las tecnologías emergentes para delinquir (IoT, cloud...) y la irrupción de nuevos debates sobre la privacidad y la legislación vigente en materia de seguridad, no ya en foros especializados, sino incluso en el día a día; en la calle.

En los siguientes epígrafes de este informe intentaremos resumir sucintamente algunos de los sucesos más relevantes que han tenido lugar en 2016, agrupándolos por categorías. Esperamos que esta lectura sea de su agrado.

5 BRECHAS DE SEGURIDAD. FUGAS DE INFORMACIÓN

Se entiende por fuga de información la transmisión no autorizada de información desde dentro de una organización a un destino externo [9]. Normalmente, esta exfiltración de información tiene lugar debido a una brecha de seguridad producida en la organización, ya sea por una intrusión, un fallo en los controles de seguridad que permite a un empleado descontento filtrar datos, un error de configuración o de programación que deja accesibles datos sensibles...

Este tipo de incidentes de seguridad son ya clásicos y llevan años produciéndose. Todo tipo de empresas y entes han sufrido alguna fuga de información y periódicamente se publican noticias en los medios sobre un nuevo caso. No obstante, el pasado 2016 tiene el dudoso honor de haber sido testigo de la mayor fuga de información de la historia: la de cuentas de usuarios de Yahoo! [10] [11].

Otro de los casos de fuga de información que más ampollas levantó durante el 2016 fue el conocido como "Papeles de Panamá" [14], en el que se filtraron datos de la contabilidad opaca de cientos de empresas y particulares.

En los siguientes puntos del informe abordaremos estos dos casos de forma más detallada. No obstante, no fueron los únicos que salieron a la luz, habiéndose reportado brechas de seguridad en compañías como LinkedIn, DropBox, Brazzers... e incluso en el sindicato del cuerpo de Mozos de Escuadra catalán [17]. Se insta al lector a visitar [16] [18] para conocer algunos otros ejemplos.

5.1 El caso Yahoo!

El pasado 22 de septiembre Bob Lord, CISO de la empresa Yahoo!, confirmaba a través del sitio oficial de la compañía en Tumblr que habían sufrido una brecha de seguridad que provocó el robo de 500 millones de cuentas de usuario [12]. Entre los datos sustraídos se encontraban nombres, direcciones de email, números de teléfono, fechas de nacimiento, el hash de las contraseñas e incluso las preguntas de seguridad de los usuarios. No obstante, afirmaba que otro tipo de información sensible como datos bancarios, no se había visto afectada.

Al parecer, las investigaciones realizadas sobre los sistemas corporativos indicaban que la brecha de seguridad se produjo en el año 2014, aunque como el lector puede comprobar, la compañía no reconoció lo sucedido hasta el 2016.

Tres meses después, el 14 de diciembre, Bob Lord volvía a emitir un comunicado en el que alertaba de un nuevo robo de información, distinto al anterior, que había afectado a 1.000 millones de cuentas de usuario [13]. En este caso las investigaciones indicaban que la brecha de seguridad se había producido en agosto de 2013.

Aunque desde Yahoo! se llegó a insinuar que tras estos hackeos estaba la figura de algún ente gubernamental, no se han aportado más detalles sobre lo sucedido ni se ha esclarecido quién es el responsable. Como ya se ha indicado, el elevado número de usuarios afectados ha llevado a los medios especializados a considerar a estas fugas de información como las mayores de la historia.

5.2 Los papeles de Panamá

Los papeles de Panamá es el nombre por el que los medios de comunicación de masas conocen una filtración de documentos confidenciales de la firma de abogados panameña Mossack Fonseca [14].

Tras una brecha de seguridad en el mencionado bufete, el periódico alemán *Süddeutsche Zeitung* recibió 2,6 terabytes de información de parte de una fuente no identificada, y posteriormente los compartió con el Consorcio Internacional de Periodistas de Investigación que se encargó de publicar la información de cientos de empresas y particulares que usaban contabilidad opaca para evadir dinero en paraísos fiscales.

La repercusión de este incidente de seguridad fue tal que aún hoy en día se publican noticias en los principales medios haciendo alusión a esta información.

Pese a que no se han publicado los detalles de la brecha de seguridad sufrida por la empresa panameña, algunos investigadores apuntan a que el hackeo pudo deberse a un plugin vulnerable del gestor de contenidos WordPress de la web de la empresa [15].

5.3 Haxposición

Estas brechas de información dejan de manifiesto el auge de una actividad que ha sido denominada haxposición por los medios especializados.

El término haxposición surge de la combinación de hacking y exposición de datos. Hace referencia al robo de datos mediante ataques informáticos y la consecuente divulgación pública o filtración de esos datos privados [19].

El término fue acuñado durante el año 2015 tras las fugas de información sucedidas en Hacking Team y Ashley Madison, cuando quedó patente que en muchas ocasiones estos hackeos tienen como motivación desprestigiar a la empresa comprometida o a sus clientes.

Se trata de una tendencia que se espera que continúe en boga en los próximos meses e incluso años, por lo que probablemente veremos más casos similares en un futuro a corto plazo.

6 CONSOLIDACIÓN DE LOS CASOS DE RANSOMWARE

A estas alturas el ransomware no necesita presentación. Todos los lectores habrán oído acerca de este malware que restringe el acceso a determinadas partes o archivos del sistema infectado y que pide un rescate a cambio de quitar esa restricción.

Aunque estrictamente existen dos categorías dentro del ransomware, bloqueadores y cifradores, la realidad es que a día de hoy la práctica totalidad de las muestras de malware analizadas por las casas antivirus se corresponden con el segundo tipo: tratan de cifrar los datos del sistema infectado.

Tal y como se vaticinó desde diversos medios, 2016 ha sido el año en el que este tipo de malware se ha consolidado como uno de los más propagados. Las infecciones por ransomware han crecido

exponencialmente en los últimos años y ya podemos hablar, sin temor a equivocarnos, de una auténtica pandemia a nivel mundial.

Para que el lector pueda hacerse una idea de las dimensiones que está alcanzando el problema, baste la siguiente infografía realizada por Kaspersky:

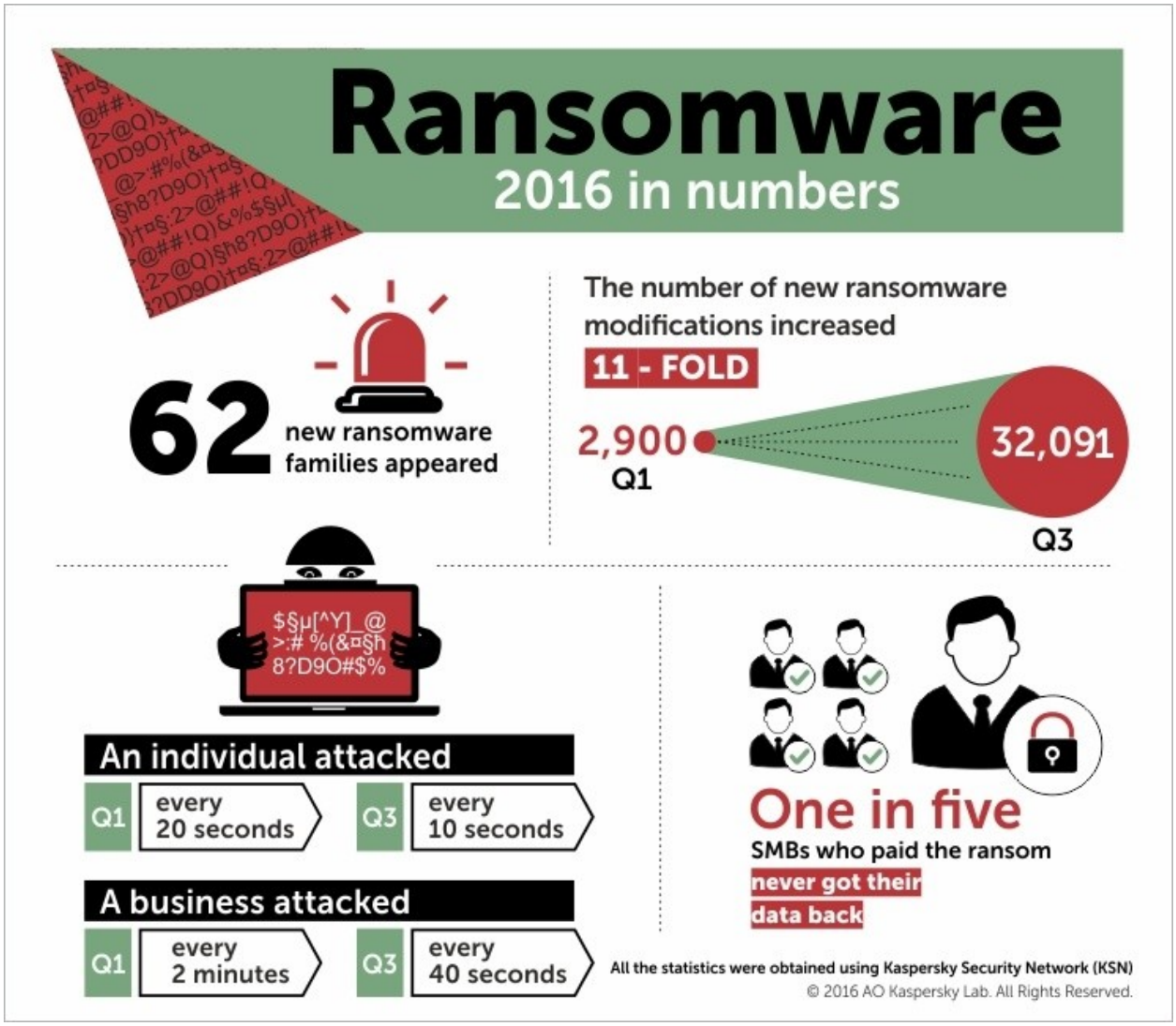

Figura 1. Infografía elaborada por Kaspersky para exponer el crecimiento del ransomware durante 2016 [21].

6.1 Situación durante el 2016: nuevas variantes, muestras más activas...

Atendiendo al estudio realizado por la firma Kaspersky [21], durante el año 2016 las familias de ransomware más activas fueron:

Nombre	Firma del motor antivirus	Porcentaje en relación al total de infecciones
CTB-Locker	Trojan-Ransom.Win32.Onion/ Trojan-Ransom.NSIS.Onion	25,32 %
Locky	Trojan-Ransom.Win32.Locky/ Trojan-Dropper.JS.Locky	7,07 %
TeslaCrypt	Trojan-Ransom.Win32.Bitman	6,54 %

Tabla 1. Pódium de las familias de ransomware con más infecciones hasta octubre de 2016 según Kaspersky.

Hay que indicar que Locky es una nueva familia de ransomware que hizo su aparición en escena precisamente durante 2016 y que afectó especialmente a España. Otras familias que han aparecido durante el pasado año son Cerber y CryptXXX. Son sólo algunos ejemplos de las miles de variantes (sí, ha leído usted bien, miles) que han sido detectadas durante 2016.

Otras dos nuevas variantes de ransomware aparecidas en 2016 han llamado la atención de los expertos debido a sus peculiaridades: Petya y Mamba [22]. En el caso de Petya, no se produce el cifrado de los ficheros del disco duro, sino que se cifra el MFT, es decir, la tabla maestra de particiones del sistema de ficheros, por lo que los datos siguen estando en el disco sin haber sido alterados, pero el usuario no puede acceder a ellos. Mamba va un paso más allá, pues realiza el cifrado del disco al completo (tanto los datos como la tabla maestra de particiones); es lo que se conoce como un ransomware de tipo FDE (*Full Disk Encryption*). Esto demuestra algo en lo que todos los expertos coinciden: el ransomware está creciendo en sofisticación, diversidad y complejidad.

No todo son malas noticias, ya que 2016 también ha supuesto el adiós a otras familias y variantes de ransomware. Es el caso de TeslaCrypt, cuyos autores decidieron cerrar su infraestructura criminal y publicar la clave maestra para descifrar los ficheros de los equipos infectados [23].

6.2 El informe Medidas de Seguridad contra Ransomware del CCN-CERT

La situación vivida en los últimos años en relación a las infecciones por ransomware, llevó al CCN-CERT, la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, a elaborar el informe "IA-01/16 Medidas de seguridad contra Ransomware", en el que dan a conocer pautas y recomendaciones de seguridad para ayudar a prevenir, gestionar y afrontar los incidentes de este tipo.

El informe, de 29 páginas, cubre tanto medidas preventivas como reactivas, restauración de ficheros y descifrado de los datos. Desde AndalucíaCERT recomendamos encarecidamente su lectura, ya que se ha convertido en una referencia a nivel mundial. El lector podrá encontrarlo en [24].

6.3 Otras iniciativas para mitigar el problema. No More Ransom! y Latch ARW

Como hemos dicho en párrafos anteriores, no todas las noticias de 2016 relacionadas con ransomware son malas. Al informe del CCN-CERT sobre este tipo de malware hay que sumar la liberación de algunas herramientas de descifrado por parte de las principales firmas antivirus[1]. De igual forma, diversos organismos, tanto públicos como privados, han aunado esfuerzos en su lucha contra este problema y han colaborado para publicar proyectos tan interesantes como *No More Ransom!*

No More Ransom! es una web elaborada por diversos cuerpos de seguridad y empresas del sector en la que se ofrecen tres funcionalidades: información sobre qué es el ransomware y cómo funciona; una herramienta para identificar el tipo de ransomware que nos ha infectado; y un repositorio de programas con los que intentar eliminar el cifrado de los datos.

La página del proyecto está disponible en [25] y, al igual que el informe del CCN-CERT, podemos asegurar que se ha convertido en una referencia a nivel mundial, por lo que se insta al lector a visitarla.

Desde AndalucíaCERT también nos gustaría hacer mención a una interesante iniciativa que ha tenido su origen en los laboratorios de la empresa Eleven Paths. Se trata de la herramienta *Latch ARW*, que mediante un control de los permisos de escritura en determinadas carpetas, pretende evitar el cifrado de los datos del equipo si se llega a producir una infección. El lector podrá encontrar más información sobre este software en [26].

7 PRINCIPALES VULNERABILIDADES PUBLICADAS

Una vulnerabilidad es un agujero de seguridad que permite, mediante su explotación, violar la seguridad del sistema.

Constantemente, los investigadores de seguridad de todo el mundo reportan las vulnerabilidades que descubren a los responsables de los sistemas, para que sean parcheados antes de hacer públicos los datos. Como se puede observar en la Figura 2, el número de vulnerabilidades descubiertas se ha disparado en los últimos años y a lo largo del 2016 se publicaron cerca de 6.500 en la base de datos con la que cuenta el NIST americano.

Diariamente, los responsables de seguridad de las distintas organizaciones deben revisar las vulnerabilidades descubiertas para aplicar los correspondientes parches en los sistemas afectados. En los siguientes puntos del informe repasaremos algunas de las vulnerabilidades más relevantes del pasado año, aunque instamos al lector a revisar otros recursos como [28] para tener una visión más completa.

1 Lamentablemente, dichas herramientas de descifrado sólo son válidas par algunas familias y variantes concretas de ransomware.

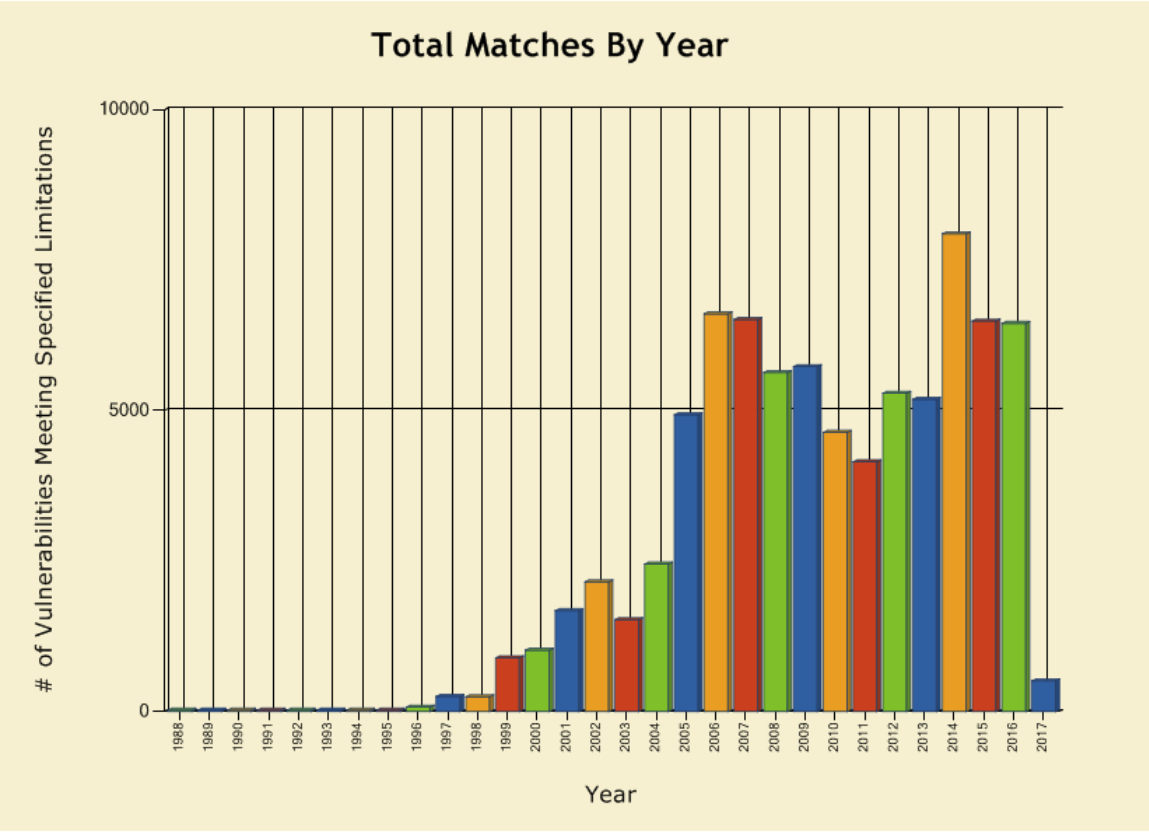

Figura 2. Evolución del número de vulnerabilidades publicadas en la base de datos del NIST [27].

7.1 Microsoft

Como bien sabrá todo el personal de IT que tenga a su cargo equipos del gigante de Redmond, Microsoft tiene una política de actualizaciones según la cual va agrupando los diferentes parches de seguridad en boletines que son liberados los segundos martes de cada mes.

A lo largo del año 2016 la firma americana publicó un total de 155 boletines de seguridad para diversos productos (sistemas operativos, paquetes ofimáticos, etc.) que han solucionado múltiples vulnerabilidades, algunas de ellas de gravedad crítica.

De entre la larga lista de vulnerabilidades corregidas, desde AndalucíaCERT queremos hacer especial mención a dos de ellas, que motivaron el envío de sendas alertas de seguridad por parte de nuestro equipo:

- Badlock. Vulnerabilidad crítica que afecta al protocolo SMB/CIFS de los sistemas Windows (así como versiones compatibles) y que permite la realización de ataques MITM y de denegación de servicio [29].

- Un par de zero-days descubiertos a finales de octubre y que estaban siendo explotados en ataques dirigidos [30].

Se insta al lector a visitar [31] para conocer el listado completo de las vulnerabilidades que han sido parcheadas por Microsoft durante el año 2016.

7.2 GNU/Linux

Lejos de lo que algunos puedan creer, el hecho de que el software sea libre (*free software*) o abierto (*open source*) no implica que esté exento de vulnerabilidades. Un claro ejemplo lo constituyen los sistemas GNU/Linux, para los que continuamente aparecen parches de seguridad (tanto para el núcleo como para los programas que se ejecutan en el sistema).

Desde AndalucíaCERT nos gustaría recordar dos vulnerabilidades del ecosistema Linux que nos forzaron a lanzar sendas alertas de seguridad:

- Ejecución remota de código en git. Vulnerabilidad de gravedad alta que permite la ejecución remota de código en el sistema afectado [32].

- DirtyCOW. Vulnerabilidad del núcleo de Linux que permite el escalado de privilegios [33].

Por supuesto, no han sido las únicas que se han descubierto y parcheado, habiéndose reportado vulnerabilidades de mayor o menor relevancia en glibc, cryptsetup, BIND, ntp...

7.3 Equipamiento de red

A lo largo del año se ha hecho público la explotación de vulnerabilidades en cortafuegos por grupos como Equation Group; un riesgo como este pone en tela de juicio la seguridad de las organizaciones.

Otros componentes como routers, switches y los diferentes *appliances* usados en cualquier red de cierto tamaño han presentado diversas vulnerabilidades que han debido ser corregidas en 2016. Nos gustaría destacar las siguientes:

- Vulnerabilidad ssh en productos de seguridad Fortinet que permite el acceso remoto al dispositivo con privilegios de root [34].

- *Buffer Overflow* en los sistemas CISCO (ASA) que afecta al sistema de intercambio de claves [35].

- Credenciales por defecto en switches Cisco Nexus 3000 y 5000. Vulnerabilidad crítica que permite el acceso remoto (telnet/ssh) a los dispositivos indicados [36].

- Múltiples vulnerabilidades críticas en productos Symantec y Norton. [37]

- Ejecución remota de código en sistemas CISCO (ASA). Vulnerabilidad presente en el código SNMP que permite a un atacante la ejecución remota de código en el sistema [38].

- *Cookie Parser Buffer Overflow*. Vulnerabilidad de algunos productos Fortinet que puede ocasionar el acceso remoto para la administración del dispositivo [39].

7.4 El entorno web

El ecosistema web ha adquirido cada vez más protagonismo en el mundo de la informática, hasta el punto de que muchas aplicaciones de escritorio se están reconvirtiendo en servicios web, por lo que no es de extrañar que cada vez observemos un mayor número de vulnerabilidades en estos entornos.

Durante 2016 se dio a conocer un nuevo ataque a la privacidad de las comunicaciones, DROWN. Se trata de una vulnerabilidad HTTPS presente en los sistemas que aún soportan el protocolo SSL v2 y que podría permitir descifrar el tráfico. El lector podrá encontrar más información al respecto en [40].

La otra gran vulnerabilidad web de 2016 fue HTTPoxy, que afecta a entornos CGI y podría permitir la ejecución remota de código [41].

Obviamente no fueron las únicas, pero sí las más afamadas. Dese AndalucíaCERT también nos gustaría nombrar las múltiples vulnerabilidades que son descubiertas constantemente en algunos de los CMS más populares, como Drupal, WordPress y Joomla! Se insta al lector a visitar [42] [43] [44] para estar al tanto de las vulnerabilidades de estos productos.

7.5 Adobe

Adobe es una de las empresas más reconocidas del sector a nivel mundial. Desde hace años su software Adobe Flash es, junto al complemento para navegadores de Java, una de las principales puertas de acceso del malware a los equipos de los usuarios.

El año 2016 no ha sido diferente y desde AndalucíaCERT nos hemos visto obligados a publicar un total de 4 alertas de seguridad avisando sobre diversas vulnerabilidades y zero-days descubiertos en Flash [45] [46] [47] [48].

Esta situación nos lleva a desaconsejar el uso de Adobe Flash. Desde AndalucíaCERT les recomendamos que no instalen este software en sus sistemas a no ser que sea estrictamente necesario. En caso de que lo tengan instalado, les recomendamos que lo mantengan desactivado y sólo lo activen en situaciones controladas.

No obstante, Flash no es el único producto desarrollado por Adobe, por lo que les recomendamos visitar [49] para conocer los problemas de seguridad que han afectado a otros programas de la compañía.

7.6 Oracle

Oracle está catalogada como la una de las mayores compañías a nivel mundial de tecnologías de la información. Aunque su principal línea de negocio son las bases de datos, comercializa otros productos entre los que se incluye el lenguaje de programación Java.

De forma parecida a lo que sucede con Microsoft, Oracle cuanta con una política de actualizaciones de seguridad según la cual va agrupando todos los parches en diversos boletines que son publicados con una periodicidad trimestral. Sugerimos al lector que visite [50] para ampliar información.

De entre todas las vulnerabilidades corregidas, además de las que afectan a Java, nos gustaría resaltar el CVE-2016-6662, que afecta al sistema gestor de bases de datos MySQL y sus derivados (MariaDB y Percona) y que podrían permitir la ejecución remota de código en los sistemas afectados. Desde AndalucíaCERT lanzamos el pasado septiembre una alerta de seguridad avisando sobre este problema [51] que requería de una actualización inmediata.

8 EL ECOSISTEMA MÓVIL

La irrupción del ecosistema móvil en el mundo de las ciberamenazas no debe suponer una sorpresa para el lector. Desde la aparición del smartphone su expansión ha sido imparable, por lo que es lógico que los delincuentes se las hayan ideado para explotar este nuevo nicho de mercado. No obstante, durante 2016 se sucedieron una serie de hitos que creemos que deben ser mencionados.

8.1 La situación del malware en Android

Tal y como menciona Kaspersky en su informe [6], la mayor parte del malware para dispositivos móviles consiste en aplicaciones de tipo advertising (adware). Esto es, su principal función es mostrar anuncios en los dispositivos infectados, obteniendo los cibercriminales un beneficio por cada anuncio visualizado[2].

No obstante, tal y como alertaba Sergio de los Santos en el pasado Webinar "*Malware en sistemas móviles. Una visión técnica y realista*" organizado por Seguridad y Confianza Digital [52], cada vez son más los malwares que buscan rootear el dispositivo que infectan para obtener mayor capacidad de acción. Esta situación está favoreciendo la aparición de malware que roba información de los terminales infectados, así como otro tipo de apps espía. En este sentido, nos gustaría resaltar al malware Gooligan, que gracias a apps maliciosas alojadas en markets no oficiales, llegaba a comprometer el dispositivo y a robar información sensible. El lector podrá encontrar más información al respecto en [61].

2 Los beneficios pueden variar dependiendo de la agresividad del anuncio. Cuanto más intrusivo y molesto para el usuario, mayor es el beneficio.

En el presente epígrafe sólo hemos mencionado el malware en Android. Aunque también existe malware para otras plataformas como iOS y Windows Phone, la realidad es que se trata de algo meramente anecdótico. La mayor parte del malware en dispositivos móviles se da para la plataforma Android.

8.2 Vía de infección. Markets no oficiales y Fake Apps

Una vez expuesta la situación del malware para terminales móviles, se debe hablar de las posibles vías de infección. ¿Cómo se llega a infectar un smartphone? Según lo observado en 2016, a día de hoy la mayor parte de las infecciones se producen gracias a la interacción del usuario, esto es, es el propio usuario quien consciente o inconscientemente autoriza la instalación de un código dañino en su dispositivo. Por ello, el uso de ingeniería social está a la orden del día [52]. Se pretende engañar al usuario para que acabe instalando alguna aplicación que realmente no presta las funcionalidades prometidas, sino que en realidad es malware.

Está claro que la mayoría de las aplicaciones con malware están alojadas en markets no oficiales y de dudosa reputación. La instalación de software desde fuentes no fiables es una de las principales vías de infección. No obstante, el market oficial para Android, Play Store, contiene gran cantidad de apps maliciosas debido a los laxos controles que impone Google para publicar en él[3]. Esto ha llevado a entidades como la Oficina de Seguridad del Internauta (OSI) a lanzar avisos sobre ciertas aplicaciones [57].

De entre todas las apps maliciosas que fueron publicadas durante 2016 en Play Store, nos gustaría mencionar a todas las apps falsas que se hacían pasar por juegos de moda, como Pokemon Go y Mario Run. Los cibercriminales aprovechaban el deseo de los usuarios por jugar con estas apps para publicar aplicaciones falsas antes de que la original hubiese salido al mercado. El lector podrá encontrar más información en [58], [59] y [60].

Figura 3. Dos de las aplicaciones falsas que aparecieron en los markets antes de su salida al mercado.

8.3 Smishing

Desde AndalucíaCERT también nos gustaría alertar sobre otro de los mayores riesgos del ecosistema móvil en la actualidad: el smishing. Se trata de un nuevo tipo de delito, muy extendido durante el año 2016, con el que se pretende trasladar el tradicional phishing recibido por e-mail al mundo de los terminales móviles.

3 Hay que ser justos y reconocer que Google también realiza una gran labor retirando del market oficial, en el menor tiempo posible, cualquier app que sea maliciosa.

Para ello, los mensajes fraudulentos son recibidos en forma de SMS o como un simple mensaje a través de los principales clientes de mensajería (WhatsApp, Line, Telegram...).

Durante el pasado 2016, entidades como la Oficina de Seguridad del Internauta (OSI) alertaron en diversas ocasiones acerca de timos relacionados con supuestos premios o mensajes solicitando credenciales al usuario en nombre de alguna entidad bancaria [53] [54] [55] [56].

Figura 4. Algunos ejemplos de smishing.

9 LOS PELIGROS DEL INTERNET DE LAS COSAS

Se entiende por IoT (Internet de las cosas) la interconexión digital de objetos cotidianos y supone la conexión a Internet de neveras, coches, prendas de vestir...

La seguridad de esta nueva tecnología emergente ha sido puesta en entredicho en numerosas ocasiones, como AndalucíaCERT expuso en uno de sus últimos informes divulgativos [62]. Y por si quedaba algún tipo de duda al respecto, durante 2016 pudimos ver cómo se producía un colapso de Internet a nivel mundial debido al ataque DDoS que estaba sufriendo la empresa Dyn, que ofrece servicios DNS a diversas empresas, debido a una botnet compuesta por dispositivos IoT.

9.1 El incidente Dyn

El viernes 21 de octubre de 2016, la infraestructura de servidores DNS de la empresa Dyn, dedicada a ofrecer servicios de resolución de nombres, sufrió un ataque de denegación de servicio distribuido que batió todos los récords conocidos hasta la fecha. La magnitud del ataque fue tal que en poco tiempo los servicios colapsaron y durante gran parte del día resultó imposible acceder a Twitter, WhatsApp, Netflix, Spotify... y otras muchas empresas a las que Dyn presta sus servicios. Sencillamente, ese día resultó imposible efectuar la resolución DNS, por lo que los usuarios de Internet no podían saber en qué dirección IP se encontraban los servidores de las distintas compañías mencionadas. El lector podrá encontrar más información en [63], [64], [65], y [66].

Como es lógico, millones de usuarios resultaron afectados y el problema acabó siendo portada de los principales medios de comunicación de masas, dejando patente una vez más la importancia de la seguridad y la fragilidad de ciertos sistemas.

Tras llevar a cabo las investigaciones pertinentes, se descubrió que el ataque había sido obra de una botnet conocida como Mirai, la cual estaba formada por miles de dispositivos IoT comprometidos, principalmente cámaras de seguridad IP y routers domésticos.

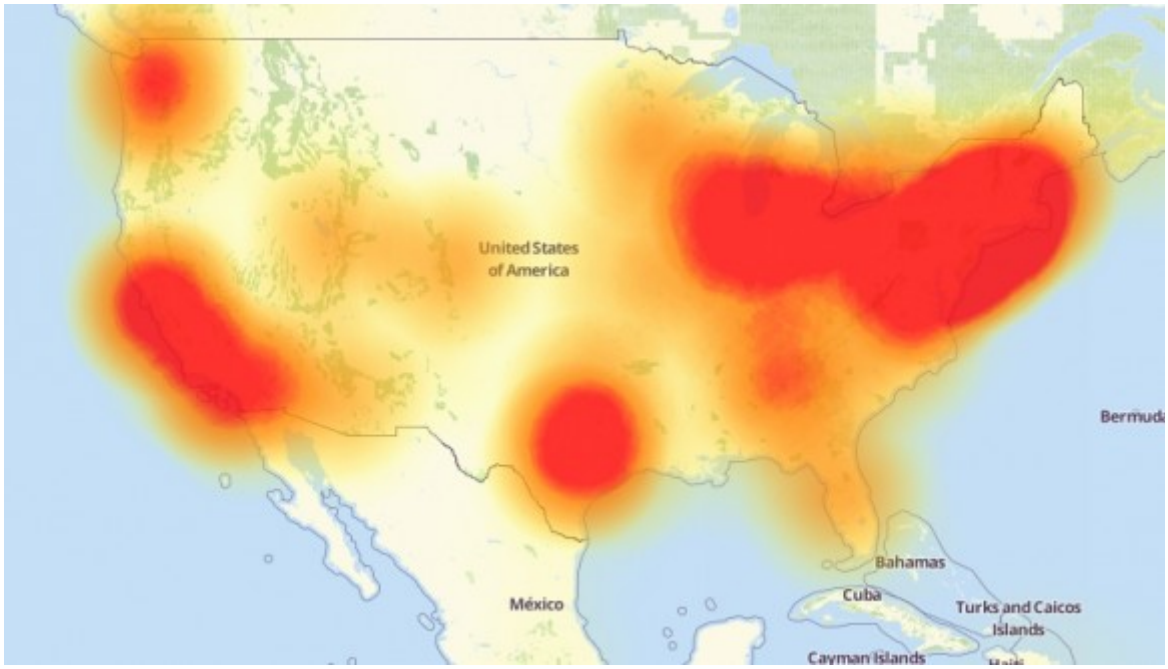

Figura 5. Descripción gráfica del ataque DDoS sufrido por los servidores de la compañía Dyn.

Este ataque no fue el primero de estas características del que se tenga constancia (véase por ejemplo el ataque sufrido por la web de Brian Krebs apenas unas semanas antes, que motivó que su proveedor de hosting se negara a seguir alojando la página [67]), no obstante, ayudó a concienciar del problema a las masas. Quedó patente el caos que supone la irrupción en Internet de miles de dispositivos vulnerables que pueden ser comprometidos y usados posteriormente para la comisión de delitos. El ciudadano de a pie comprendió que esta situación también podía afectarle directamente.

10 APTS Y NUEVOS ACTORES EN EL PANORAMA INTERNACIONAL

Tradicionalmente, las acciones criminales en la Red estaban perpetradas por una serie de actores bien conocidos que coexistían en el ciberespacio: script kiddies, hacktivistas, cibercriminales... Esta situación ha sufrido un cambio drástico en los últimos años, con la llegada de grupos supuestamente amparados por oficinas gubernamentales y el uso de APTs y ciertos malwares con características muy avanzadas.

Los gobiernos de las principales potencias han comprendido que el ciberespacio es un nuevo campo de batalla y actualmente se libra una guerra encarnizada entre diversos países. Durante 2016 hemos visto un nuevo capítulo de esta particular "guerra fría" en la que Rusia y Estados Unidos se están convirtiendo en protagonistas.

10.1 La aparición en escena de ShadowBrokers

En agosto de 2016, la cuenta de Twitter @theshadowbrokerss anunciaba que ponía en venta un arsenal de APTs usadas por Equation Group, un grupo de cibercriminales que lleva años organizando ataques dirigidos y que, supuestamente, cuenta con el amparo de la NSA americana[4].

Según parece, The Shadow Brokers habría logrado infiltrarse en los servidores usados por Equation Group para realizar sus operaciones y hacerse con algunas de las ciberarmas con las que cuentan. Para dar veracidad a esta filtración, publicaron de forma gratuita algunas de esas armas.

Para sorpresa de todos, cuando los expertos comenzaron a analizar la información filtrada comprobaron que las ciberarmas publicadas eran reales y usaban diversas vulnerabilidades y zero-days para explotar los sistemas. Más aún, la firma Kaspersky, que fue la primera en identificar las acciones llevadas a cabo por Equation Group, aseguró que se trataba de los mismos exploits y malwares que ellos habían estudiado con anterioridad y de los que tenían algunas muestras.

A día de hoy se especula con la posibilidad de que el grupo The Shadow Brokers haya sido patrocinado por el gobierno ruso, con el fin de dar un toque de atención a los Estados Unidos y hacerles ver que son conscientes de las acciones de espionaje que están llevando a cabo y que no piensan consentirlo.

El lector podrá encontrar más información sobre The Shadow Brokers en [68] y [69]. De igual forma, se recomienda la lectura de [70] para conocer más a fondo las operaciones llevadas a cabo por Equation Group.

10.2 Fancy Bears y las filtraciones de la Agencia Mundial Antidopaje

El grupo criminal Fancy Bear no supone una novedad en el panorama internacional. Llevan años realizando ataques dirigidos y se especula con la posibilidad de que estén patrocinados por alguna agencia del gobierno ruso. Durante 2016 pudimos ser testigos de otra de sus actuaciones: las filtraciones de información de la Agencia Mundial Antidopaje.

Como bien recordará el lector, la participación de deportistas rusos en los pasados Juegos Olímpicos de Río estuvo a punto de ser vetada por el COI debido a una supuesta red de dopaje [72]. Este hecho motivó que el grupo Fancy Bears hackease a la Agencia Mundial Antidopaje y comenzara a filtrar información sobre el supuesto dopaje encubierto de algunas estrellas del deporte como Simone Biles y las hemanas Williams [71].

Obviamente, estas filtraciones tuvieron mucha repercusión en los medios de información de masas, generando cierta polémica acerca de los permisos médicos que recibieron esos atletas para tomar determinadas sustancias que en condiciones normales están prohibidas.

4 No faltan voces, entre otras la de Edward Snowden, que apuntan a que Equation Group es una división de la NSA usada para realizar operaciones de ciberespionaje en la Red.

Por otra parte, y al igual que en otras operaciones similares, se especuló con que el gobierno ruso estaba detrás de lo sucedido. En esta ocasión, como venganza por el veto a sus deportistas.

10.3 El hackeo de las elecciones presidenciales en Estados Unidos

La guinda del pastel de esta particular "guerra fría" llegó durante las pasadas elecciones presidenciales en los Estados Unidos de América. Supuestamente, el gobierno ruso llevó a cabo diversos ataques cibernéticos para interferir en las elecciones y apoyar al candidato Donald Trump, dada su afinidad con el presidente ruso Vladimir Putin.

Estos hechos llevaron al ya expresidente Barack Obama a emprender una serie de sanciones contra Rusia, como la expulsión inmediata de 35 diplomáticos rusos de suelo estadounidense [73].

11 ATAQUES CONTRA INFRAESTRUCTURAS CRÍTICAS

Se entiende por infraestructuras críticas aquellas consideradas como estratégicas para un país, las que prestan servicios esenciales a la sociedad, pero cuya sustitución o reemplazo no presenta alternativa posible. Algunos ejemplos serían los sistemas de suministro de agua y electricidad, el sector de las finanzas y los medios de pago, el sector sanitario... Se insta al lector a visitar [74] y [75] para tener una visión más completa sobre las infraestructuras críticas.

Dada la importancia de este tipo de sistemas, es lógico que se hayan convertido en uno de los principales objetivos de los cibercriminales (e incluso de algunos grupos patrocinados por gobiernos, con el objetivo de realizar actos de ciberguerra). El pasado 2016 nos brindó algunos ejemplos de ciberataques sufridos por infraestructuras críticas en diversas partes del mundo. A continuación comentaremos algunos de los más sonados.

11.1 Ciberataque contra la red eléctrica ucraniana

Durante la Navidad de 2015 un fallo en la red eléctrica de la región Ivano-Frankivsk en Ucrania interrumpió el suministro en más de 600.000 hogares. No fue hasta principios de 2016 cuando se comenzaron a hacer públicas las conclusiones obtenidas gracias a las investigaciones realizadas: se trató de un ciberataque causado por el troyano BlackEnergy. Se insta al lector a consultar [76] para conocer más detalles sobre lo sucedido.

Desde la aparición del malware Stuxnet en el año 2010, los expertos en seguridad a nivel mundial ya saben que los sistemas industriales y SCADA son un objetivo más que puede ser atacado. El incidente de Ucrania volvió a dejarlo patente, pero lejos de haber sido algo puntual, hace apenas unos días desde el CERTSI avisaban de otro posible ciberataque contra la red eléctrica de Ucrania [77].

11.2 Atracos bancarios virtuales usando SWIFT

Otra de las noticias más impactantes de 2016 fueron los diversos robos que se produjeron en entidades bancarias aprovechando vulnerabilidades presentes en el sistema SWIFT, usado para regir las transacciones de dinero a nivel internacional.

Un claro ejemplo fueron los 81 millones de dólares que se sustrajeron de diversas cuentas del Bangladesh Bank en febrero de 2016. El lector podrá encontrar más información en [78]. No fueron los únicos casos observados durante 2016, ya que también se reportaron ataques contra cajeros automáticos de diversas entidades.

Estos hechos han expuesto al mundo las debilidades del sistema SWIFT y han demostrado que en la actualidad no hacen falta una media y una pistola para atracar un banco. Basta con tener conocimientos informáticos e intenciones delictivas.

11.3 El sector sanitario, en el punto de mira

Uno de los sectores que más incidentes ha sufrido durante el pasado 2016 es el sanitario. Los ciberdelincuentes han comprendido que la importancia de los activos que manejan organizaciones como los hospitales puede reportarles jugosos beneficios, por lo que los han colocado en el centro de su diana.

En particular, durante 2016 se observaron multitud de ataques de tipo ransomware cuyo objetivo eran precisamente los datos almacenados en sistemas hospitalarios. El lector podrá encontrar algunas referencias en [79], [80] y [81]. Está claro que, si bien un usuario doméstico puede permitirse perder datos ya que no son importantes, para un hospital la pérdida de los datos médicos de sus pacientes puede ser algo de vida o muerte, de ahí su importancia y que algunos centros estén dispuestos a pagar para recuperar dichos datos y para que estos ataques cesen.

No obstante, ese no es el único problema que atañe al sector sanitario. El uso de multitud de aparatos y maquinaría que comienzan a ofrecer funciones que necesitan de una conexión en red (ecógrafos, máquinas de rayos, sistemas de monitorización de constantes vitales...) está generando todo tipo de problemas debido a la escasa seguridad con la que cuentan dichos dispositivos y las vulnerabilidades que les son descubiertas. El lector podrá encontrar información al respecto en [82].

Figura 6. Equipamiento médico de última generación, con posibilidad de comunicación en red.

12 DEBATE PRIVACIDAD/SEGURIDAD

La existencia de un acalorado debate sobre la privacidad de la información y los límites que se les debería imponer a gobiernos y empresas a la hora de recabar información sobre los usuarios, no debería suponer una novedad para el lector. Todos llevamos años discutiendo sobre el tema.

A lo largo de 2016 hemos observado algunos sucesos que han conseguido reavivar este debate. A continuación resumimos sucintamente algunos de esos hechos.

12.1 El iPhone del terrorista de San Bernardino

El 2 de diciembre de 2015 se produjo un ataque terrorista en la localidad californiana de San Bernardino. Tras un tiroteo llevado a cabo contra civiles, el atentado se saldó con 14 personas muertas y otras 21 heridas.

Durante las investigaciones llevadas a cabo por el FBI, una de las principales pruebas resultó ser un smartphone modelo iPhone 5c propiedad de uno de los autores del tiroteo. No obstante, todos los datos que contenía estaban cifrados, por lo que no podían acceder a ellos.

Desde el FBI se solicitó la colaboración de la compañía Apple para que ayudase a descifrar la información y, para sorpresa de muchos, la empresa de la manzana se negó a colaborar aduciendo que debía respetar la privacidad de sus usuarios, incluso si alguno de ellos era un presunto terrorista.

La decisión de Apple abrió un enorme debate en la sociedad norteamericana (y por extensión, en el resto del mundo) e incluso el Departamento de Justicia de los Estados Unidos llegó a amenazar a la empresa con una demanda por obstrucción. No obstante, dicha demanda nunca llegó a hacerse efectiva, puesto que unos días después el FBI anunció que había conseguido descifrar el iPhone gracias a la ayuda de un tercero.

Este caso puso nuevamente en tela de juicio hasta dónde se debe preservar la privacidad de una persona y en qué casos deben existir excepciones. Por otro lado, también dejó patente la existencia de exploits y zero-days para dispositivos iPhone (ya que de otra manera hubiera resultado imposible descifrar los datos del teléfono). Se especula que el FBI llegó a pagar más de 1 millón de dólares por lograr descifrar la información. Se insta al lector a visitar [83], [84] y [85] para conocer más detalles.

12.2 El cambio de políticas de privacidad en WhatsApp

En agosto del pasado año pudimos asistir a otro de los hechos más comentados sobre la privacidad de los usuarios y las políticas un tanto intrusivas de ciertas compañías. Desde Facebook, propietario de la aplicación de mensajería instantánea WhatsApp, lanzaron una actualización de los términos y condiciones de uso del servicio para poder compartir datos entre ambas plataformas (Facebook y WhatsApp).

Figura 7. Cesión de datos de usuario entre las plataformas WhatsApp y Facebook.

Este hecho motivó que la Oficina de Seguridad del Internauta lanzara un aviso informativo [86] y obligó a que la Agencia Española de Protección de Datos comenzara a investigar si esta cesión de datos personales de los usuarios era legal [87].

13 ¿SE CUMPLIERON LAS PREDICCIONES DEL AÑO ANTERIOR?

Una vez desglosados los principales hitos del mundo de la Seguridad de la Información durante el año 2016, nos quedaría echar la vista atrás y comprobar si se cumplieron las predicciones realizadas por AndalucíaCERT en su "Informe de divulgación. Predicciones sobre amenazas para 2016" [88]. Y como el lector podrá comprobar simplemente haciendo una comparación, las predicciones se han cumplido en su práctica totalidad.

Todo apuntaba a que ciertos pronósticos, como el auge del ransomware, los peligros del IoT y el aumento de los ataques contra infraestructuras críticas se verían cumplidos. No sólo AndalucíaCERT alertó sobre ello, sino otros muchos medios especializados.

Más difícil resultaba acertar con otras predicciones, como el incremento de los ataques dirigidos y las fugas de información, así como la situación que presenta actualmente el mundo de los dispositivos móviles. No obstante, dichas predicciones también se han cumplido al 100%.

El único punto en el que se puede decir que nuestro informe falló, fue en la entrada en escena de drones para la realización de ciertos ataques. No obstante, podemos argumentar a nuestro favor que desde diversas instituciones se aunó esfuerzos para legislar sobre el tema, impidiendo que algunas de nuestras predicciones llegara a materializarse.

14 GLOSARIO

adware: Acrónimo de *advertising-supported software*. Software que automáticamente muestra u ofrece publicidad con el fin de generar lucro a sus autores.

app: Contracción de *application* (aplicación en inglés). Suele hacer referencia a las aplicaciones especialmente diseñadas para teléfonos móviles inteligentes.

appliance: Computador con un firmware o software específicamente diseñado para proporcionar un servicio o recurso concreto.

APT: Siglas de la expresión inglesa *Advanced Persistent Threat*. En español, Amenaza Persistente Avanzada. Conjunto de procesos informáticos, sigilosos y continuos, dirigidos a penetrar la seguridad de una entidad específica.

BIND: Siglas de la expresión *Berkeley Internet Name Domain*. Se trata del servidor DNS (resolución de nombres de dominio) más usado en Internet.

botnet: Conjunto de máquinas infectadas por malware que son usadas de forma automática y conjunta para la realización de acciones criminales.

Buffer Overflow: En español, desbordamiento de buffer. Se trata de un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada (el buffer).

CERTSI: Acrónimo de *CERT de Seguridad e Industria*. Se trata de la Capacidad de Respuesta a incidentes de Seguridad de la Información del Ministerio de Energía, Turismo y Agenda Digital y del Ministerio del Interior. Se encarga de la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas.

CGI: Siglas de la expresión inglesa *Common Gateway Interface*. Se trata de una tecnología web que permite a un cliente solicitar datos de un programa ejecutado en un servidor web. Por tanto, detalla la comunicación entre el servidor web y una aplicación externa que ejecuta los datos del cliente.

CIFS: Siglas de la expresión inglesa *Common Internet File System*. Protocolo de nivel de red usado principalmente para proveer acceso compartido a ficheros. Antiguamente se denominaba SMB y existe una versión libre denominada SAMBA.

cloud: Paradigma que permite ofrecer servicios de computación a través de una red.

CMS: Siglas de la expresión inglesa *Content Management System*. En español, sistema de gestión de contenidos. Se trata de un programa informático para crear un estructura de soporte para la creación y administración de páginas web.

COI: Siglas de *Comité Olímpico Internacional*. Organismo encargado de promover el olimpismo en el mundo y coordinar las actividades del Movimiento Olímpico.

Cookie: Pequeña porción de información enviada por un sitio web y almacenada en el navegador del usuario.

cryptsetup: Componente de los sistemas GNU/Linux que provee cifrado transparente de dispositivos en bloque.

DDoS: Siglas de la expresión inglesa *Distributed Denial of Service*. Se trata de un ataque a un sistema que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

dirección IP: Número que identifica de manera lógica y jerárquica a una interfaz en red. Por hacer una analogía, sería como el número de teléfono de nuestro PC.

DNS: Siglas de la expresión inglesa *Domain Name System*. Sistema de nomenclatura jerárquico para dispositivos conectados a redes IP como Internet. Su principal función es la traducción de nombres de dominio a direcciones Ips.

FBI: Siglas de *Federal Bureau of Investigation*. Se trata de la principal rama de investigación criminal del Departamento de Justicia de los Estados Unidos de América.

FDE: Siglas de la expresión inglesa *Full Disk Encryption*. Característica de algunos malwares de tipo ransomware, que cifra el disco duro del sistema infectado al completo, tanto los archivos como la tabla de particiones.

fuga de información: Se entiende por fuga de información la transmisión no autorizada de información desde dentro de una organización a un destino externo.

git: Software de control de versiones diseñado por Linus Torvalds.

glibc: Biblioteca estándar del lenguaje C de los sistemas GNU/Linux. En esta biblioteca se proporcionan y definen las llamadas al sistema y otras funciones básicas.

hacktivista: Acrónimo de *hacker* y activista. Se entiende por hacktivista aquella persona que usa herramientas digitales (legales, ilegales o legalmente ambiguas) persiguiendo fines políticos.

hash: Función resumen o *digest*. Hace uso de funciones matemáticas para generar un resumen o huella de tamaño fijo, de un recurso de tamaño arbitrario. Su bondad reside en que un mismo recurso siempre generará la misma huella y una pequeña modificación del mismo resultará en una huella completamente distinta. Además, las funciones *hash* no son reversibles, esto es, partiendo de una huella digital, nunca será posible obtener el recurso del que se ha obtenido dicha huella.

haxposición: Consiste en el robo de datos mediante ataques informáticos y la consecuente divulgación pública o filtración de esos datos privados.

hosting: Almacenamiento web.

HTTPS: Siglas de la expresión inglesa *HyperText Transfer Protocol Secure*. Protocolo de aplicación destinado a la transferencia segura de datos de hipertexto. Es la versión segura del protocolo HTTP.

infraestructuras críticas: Aquellas consideradas como estratégicas para un país, las que prestan servicios esenciales a la sociedad, pero cuya sustitución o reemplazo no presenta alternativa posible.

ingeniería social: Práctica consistente en obtener información confidencial a través de la manipulación de usuarios legítimos.

IoT: Siglas de la expresión inglesa *Internet of Things*. Concepto que se refiere a la interconexión digital de objetos cotidianos como neveras, prendas de vestir, mobiliario público...

IT: Siglas de la expresión inglesa *Information Technology*. Como su nombre indica, hace referencia a las tecnologías de la información. En español se suelen usar las siglas TI y TIC.

market: Repositorio de aplicaciones para dispositivos móviles. Aunque existen diversos tipos, sólo se recomienda el uso de aquellos que sean oficiales, como Google Play y App Store.

MFT: Siglas de la expresión inglesa *Master File Table*. Se trata de la tabla de particiones de un sistema de archivos NTFS (es decir, de sistemas Microsoft Windows).

MITM: Siglas de la expresión inglesa *Man In The Middle*. Tipo de ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

NIST: Siglas de la expresión inglesa *National Institute of Standards and Technology*. Ente del gobierno americano cuya misión es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología.

NSA: Siglas de la expresión inglesa *National Security Agency*. Se trata de la Agencia de Seguridad Nacional de los Estados Unidos de América, que forma parte de los Servicios de Inteligencia de dicho país y se encarga de llevar a cabo operaciones de espionaje y contrainteligencia.

ntp: Siglas de la expresión *Network Time Protocol*. Se trata de un protocolo de Internet usado para sincronizar los relojes de los sistemas informáticos.

phishing: Ataque de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

plugin: También conocido como complemento. Se trata de una aplicación que se relaciona con otra para aportarle una nueva función, generalmente muy específica.

ransomware: Malware que restringe el acceso a determinadas partes o archivos del sistema infectado para pedir un rescate a cambio de quitar esa restricción.

rootear: Del inglés root. Acción mediante la que se manipula el sistema operativo Android de un dispositivo móvil para obtener los máximos privilegios.

router: Dispositivo de red que proporciona conectividad mediante el envío o encaminamiento de los paquetes que recibe desde una red a otra.

SAMBA: Implementación libre del protocolo de red CIFS de los sistemas Microsoft Windows.

SCADA: Acrónimo de *Supervisory Control And Data Acquisition*. En español, Supervisión, Control y Adquisición de Datos. Concepto empleado para los sistemas que permiten controlar y supervisar procesos industriales a distancia.

script kiddie: Persona falta de habilidades técnicas, que se limita a ejecutar herramientas creadas por un tercero para llevara acabo una determinada acción, aunque realmente no comprenda el funcionamiento de la misma.

smartphone: Teléfono móvil inteligente o de última generación.

SMB: Siglas de la expresión inglesa *Server Message Block*. Se trata del nombre con el que se designaba antiguamente al protocolo CIFS.

smishing: Contracción de SMS y phishing. Variante del phishing en el que se usan mensajes de texto dirigidos a los usuarios de telefonía móvil.

SMS: Acrónimo de la expresión inglesa *Short Message Service*. Sistema de mensajes de texto para teléfonos móviles.

SNMP: Siglas de la expresión inglesa *Simple Network Management Protocol*. Protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

SPAM: También conocido como correo basura. Hace referencia a los mensajes de correo electrónico no solicitados, no deseados o con remitente no conocido, habitualmente de tipo publicitario, que son enviados en grandes cantidades y perjudican de alguna o varias maneras al receptor.

ssh: Acrónimo de la expresión inglesa *Secure Shell*. Hace referencia tanto al protocolo de comunicaciones como al programa que se usa para acceder a máquinas remotas a través de una red.

SSL: Siglas de *Secure Sockets Layer*. Protocolos criptográficos que proporcionan comunicaciones seguras por una red. Se trata del antecesor de TLS (*Transport Layer Security*).

SWIFT: Sirve para definir tanto al código de identificación bancaria usado para facilitar las transferencias internacionales de dinero, como a la sociedad internacional que actúa como consorcio y se encarga de operar la red telecomunicaciones que permite dichas transacciones.

switch: Dispositivo de red que proporciona conectividad interconectando dos o más segmentos de una misma red.

telnet: Acrónimo de la expresión inglesa *Telecommunication Network*. Se trata de un protocolo mediante el que podemos acceder a otra máquina y manejarla remotamente.

vulnerabilidad: Agujero de seguridad que permite, mediante su explotación, violar la seguridad del sistema afectado.

zero-day: Expresión inglesa por la que se conocen las vulnerabilidades software no conocidas, ya que no han sido reportadas públicamente, y que son usadas por los cibercriminales para lograr la explotación de sistemas.

15 DOCUMENTACIÓN DE REFERENCIA

[1] Antonio Ropero. <<*Resumen de seguridad de 2016 (I). Enero - Marzo*>>. Una al día. Hispasec, diciembre de 2016. Disponible en línea: http://unaaldia.hispasec.com/2016/12/resumen-de-seguridad-de-2016-i.html (Fecha de consulta, 17/01/2017).

[2] Antonio Ropero. <<*Resumen de seguridad de 2016 (II). Abril - Junio*>>. Una al día. Hispsec, diciembre de 2016. Disponible en línea: http://unaaldia.hispasec.com/2016/12/resumen-de-seguridad-de-2016-ii.html (Fecha de consulta, 17/01/2017).

[3] Antonio Ropero. <<*Resumen de seguridad de 2016 (III). Julio – Septiembre*>>. Una al día. Hispasec, diciembre de 2016. Disponible en línea: http://unaaldia.hispasec.com/2016/12/resumen-de-seguridad-de-2016-iii.html (Fecha de consulta, 17/01/2017).

[4] Antonio Ropero. <<*Resumen de seguridad de 2016 (y IV). Octubre – Diciembre*>>. Una al día. Hispasec, enero de 2017. Disponible en línea: http://unaaldia.hispasec.com/2017/01/resumen-de-seguridad-de-2016-y-iv.html (Fecha de consulta, 17/01/2017).

[5] Personal de ESET. <<*Ranking de las peores amenazas de seguridad de 2016*>>. Centro de prensa de ESET, diciembre de 2016. Disponible en línea: http://noticias.eset.es/ranking-de-las-peores-amenazas-de-seguridad-de-2016 (Fecha de consulta, 17/01/2017).

[6] David Emm, Roman Unuchk & Kirill Kruglov. <<*Kaspersky Security Bulletin 2016. Review of the year*>>. Kaspersky Lab, diciembre de 2016. Disponible en línea: https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Review_ENG.pdf (Fecha de consulta, 18/01/2017).

[7] Eduardo Medina. <<*Los trece peores incidentes de seguridad en 2016*>>. MuySeguridad .NET, diciembre de 2016. Disponible en línea: http://muyseguridad.net/2016/12/30/seguridad-en-2016/ (Fecha de consulta, 17/01/2017).

[8] Drew Milan. <<*The F5 Security Top 16 of 2016*>>. F5 Blog, diciembre de 2016. Disponible en línea: https://f5.com/es/about-us/blog/articles/the-f5-security-top-16-of-2016-24413 (Fecha de consulta, 19/01/2017).

[9] Peter Gordon. <<*Data Leakage – Threats and Mitigation*>>. SANS Institute. InfoSec Reading Room, octubre de 2007. Disponible en línea: https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931 (Fecha de consulta, 19/01/2017).

[10] Editores de ComputerWorld. <<*Yahoo sufre la mayor fuga de datos de la historia*>>. ComputerWorld, diciembre de 2016. Disponible en línea: http://cso.computerworld.es/alertas/yahoo-sufre-la-mayor-fuga-de-datos-de-la-historia (Fecha de consulta, 19/01/2017).

[11] Editores de Wikipedia. <<*Yahoo! data breaches*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://en.wikipedia.org/wiki/Yahoo!_data_breaches (Fecha de consulta, 19/01/2017).

[12] Bob Lord. <<*An Important Message About Yahoo User Security*>>. Yahoo! Tumblr Site, septiembre de 2016. Disponible en línea: https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security (Fecha de consulta 19/01/2017).

[13] Bob Lord. <<*Important Security Information for Yahoo Users*>>. Yahoo! Tumblr Site, diciembre de 2016. Disponible en línea: https://yahoo.tumblr.com/post/154479236569/important-security-information-for-yahoo-users (Fecha de consulta, 19/01/2017).

[14] Editores de Wikipedia. <<*Panama Papers*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://es.wikipedia.org/wiki/Panama_Papers (Fecha de consulta, 19/01/2017).

[15] Eduardo Medina. <<*Un plugin de WordPress puede ser el origen del ataque a Mossack Fonseca*>> MuySeguridad .NET, abril de 2016.Disponible en línea: http://muyseguridad.net/2016/04/11/plugin-wordpress-ataque-mossack-fonseca/ (Fecha de consulta, 19/01/2017).

[16] Personal de Eleven Paths. <<*Cybersecurity Shot. Investigations about data leaks*>>. Eleven Paths, 2016. Disponible en línea: https://www.elevenpaths.com/es/noticias-y-eventos/cybersecurity-shot/index.html (Fecha de consulta, 19/01/2017).

[17] Personal de Eleven Paths. <<*Fuga de información de los Mossos D'Escuadra*>>. Eleven Paths, junio de 2016. Disponible en línea: https://www.elevenpaths.com/es/informe-de-investigacion-fuga-de-informacion-de-mossos-desquadra/index.html (Fecha de consulta, 19/01/2017).

[18] Christina Schubert. <<*Data Breaches That Made Headlines in 2016*>>. Norton Protection Blog. Norton Community, diciembre de 2016. Disponible en línea: https://community.norton.com/en/blogs/norton-protection-blog/data-breaches-made-headlines-2016 (Fecha de consulta, 19/01/2017).

[19] Sabrina Pagnotta. <<*¿Sabes qué es la haxposición? Conoce a esta amenaza emergente*>>. WeliveSecurity. ESET, febrero de 2016. Disponible en línea: http://www.welivesecurity.com/la-es/2016/02/10/que-es-haxposicion-amenaza-emergente/ (Fecha de consulta, 19/01/2017).

[20] Editores de Wikipedia. <<*Ransomware*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://es.wikipedia.org/wiki/Ransomware (Fecha de consulta, 19/01/2017).

[21] Personal de Kaspersky. <<*Story of the year: The ransomware revolution*>>. Kaspersky Security Bulletin 2016. Disponible en línea: https://securelist.com/files/2016/12/KSB2016_Story_of_the_Year_ENG.pdf (Fecha de consulta, 19/01/2017).

[22] Pierluigi Paganini. <<*A Brazilian Infosec research group, Morphus Labs, just discovered a new Full Disk Encryption (FDE) Ransomware this week, dubbed Mamba*>>. SecurityAffairs, septiembre de 2016. Disponible en línea: http://securityaffairs.co/wordpress/51314/malware/mamba-ransomware.html (Fecha de consulta, 19/01/2017).

[23] Lawrence Abrams. <<*TeslaCrypt shuts down and Releases Master Decryption Key*>>. Bleeping Computer, mayo de 2016. Disponible en línea: https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/ (Fecha de consulta, 19/01/2017).

[24] Personal del CCN-CERT. <<*Informe de Amenazas CCN-CERT IA-01/16. Medidas de seguridad contra el ransomware*>> Web oficial del CCN-CERT, 2016. Disponible en línea: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1384-ccn-cert-ia-01-16-medidas-de-seguridad-contra-ransomware/file.html (Fecha de consulta, 19/01/2017).

[25] Colaboradores del proyecto NoMoreRansom! <<*No More Ranswom!*>>. Web oficial del proyecto NoMoreRansom! Disponible en línea: https://www.nomoreransom.org/ (Fecha de consulta, 19/01/2017).

[26] Personal de Eleven Paths. <<*Antiransomware*>>. Web oficial de Eleven Paths, octubre de 2016. Disponible en línea: https://www.elevenpaths.com/es/labstools/antiransomware-2/index.html (Fecha de consulta (19/01/2017).

[27] Personal del NIST. <<*CVE and CCE Statistics Query Page*>>. National Vulnerability Database. Disponible en línea: https://web.nvd.nist.gov/view/vuln/statistics (Fecha de consulta, 20/01/207).

[28] Personal de Flexera. <<*Secunia Research Community*>>. Flexera Software, 2017. Disponible en línea: https://secunia.com/community/advisories/ (Fecha de consulta, 20/01/2017).

[29] Personal de AndalucíaCERT. <<*Vulnerabilidad Badlock en Sistemas Windows y Samba*>>. Web oficial de AndalucíaCERT, abril de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-badlock-en-sistemas-windows-y-samba (Fecha de consulta, 20/01/2017).

[30] Personal de AndalucíaCERT. <<*Vulnerabilidades críticas en Microsoft Windows*>>. Web oficial de AndalucíaCERT, noviembre de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidades-criticas-en-microsoft-windows (Fecha de consulta, 20/01/2016).

[31] Personal de Microsoft. <<*Security Bulletins 2016*>>. Microsoft Security TechCenter, 2016. Disponible en línea: https://technet.microsoft.com/en-us/library/security/mt637763.aspx (Fecha de consulta, 20/01/2017).

[32] Personal de AndalucíaCERT. <<*Vulnerabilidad en el sistema de control de versiones git*>>. Web oficial de AndalucíaCERT, marzo de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-en-el-sistema-de-control-de-versiones-git (Fecha de consulta, 20/01/2017).

[33] Personal de AndalucíaCERT. <<*Vulnerabilidad en el kernel de Linux (DIRTY COW)*>>. Web oficial de AndalucíaCERT, octubre de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-en-el-kernel-de-linux-dirty-cow (Fecha de consulta, 20/01/2017).

[34] Personal de AndalucíaCERT. <<*Vulnerabilad SSH en productos de seguridad Fortinet*>>. Web oficial de AndalucíaCERT, enero de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilad-ssh-en-productos-de-seguridad-fortinet (Fecha de consulta, 20/01/2017).

[35] Personal de AndalucíaCERT. <<*Vulnerabilidad en sistemas Cisco (ASA)*>>. Web oficial de AndalucíaCERT, febrero de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-en-sistemas-cisco-asa (Fecha de consulta, 20/01/2017).

[36] Personal de AndalucíaCERT. <<*Vulnerabilidad de credenciales por defecto en switches Cisco Nexus 3000 y 3500*>>. Web oficial de AndalucíaCERT, marzo de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-de-credenciales-por-defecto-en-switches-cisco-nexus-3000 (Fecha de consulta, 20/01/2017).

[37] Personal de AndalucíaCERT. <<*Vulnerabilidades críticas en productos Symantec y Norton*>>. Web oficial de AndalucíaCERT, junio de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidades-criticas-en-productos-symantec-y-norton (Fecha de consulta, 20/01/2017).

[38] Personal de AndalucíaCERT. <<*Vulnerabilidad en sistemas Cisco (ASA)*>>. Web oficial de AndalucíaCERT, agosto de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-en-sistemas-cisco-asa-0 (Fecha de consulta, 20/01/2017).

[39] Personal de AndalucíaCERT. <<*Vulnerabilidad en sistemas Fortinet*>>. Web oficial de AndalucíaCERT, agosto de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-en-sistemas-fortinet (Fecha de consulta, 20/01/2017).

[40] Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky y otros. <<*DROWN: Breaking TLS using SSLv2*>>. Página web oficial de la vulnerabilidad DROWN, julio de 2016. Disponible en línea: https://drownattack.com/ (Fecha de consulta 24/01/2017).

[41] Dominic Scheirlinck y el equipo de investigadores que descubrió HTTPoxy. <<*HTTPoxy. A CGI application vulnerability for PHP, Go, Python and other*>>. Página web oficial de la vulnerabilidad HTTPoxy, agosto de 2016. Disponible en línea: https://httpoxy.org/ (Fecha de consulta, 24/01/2017).

[42] Equipo de seguridad de Drupal. <<*Drupal Security Advisories*>>. Página web oficial del proyecto Drupal. Disponible en línea: https://www.drupal.org/security (Fecha de consulta, 24/01/2017).

[43] Equipo de seguridad de WordPress. <<*WordPress Security Category Archive*>>. Página web oficial del proyecto WordPress. Disponible en línea: https://wordpress.org/news/category/security/ (Fecha de consulta, 24/01/2017).

[44] Equipo de seguridad de Joomla! <<*Joomla! Security Announcements*>>. Página web oficial del proyecto Joomla! Disponible en línea: https://developer.joomla.org/security-centre.html (Fecha de consulta, 24/01/2017).

[45] Personal de AndalucíaCERT. <<*Vulnerabilidad crítica en Adobe Flash Player - 0day*>>. Web oficial de AndalucíaCERT, mayo de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-critica-en-adobe-flash-player-0day (Fecha de consulta, 24/01/2017).

[46] Personal de AndalucíaCERT. <<*Vulnerabilidad crítica en Adobe Flash Player*>>. Web oficial de AndalucíaCERT, junio de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-critica-en-adobe-flash-player (Fecha de consulta, 24/01/2017).

[47] Personal de AndalucíaCERT. <<*Vulnerabilidad crítica en Adobe Flash Player*>>. Web oficial de AndalucíaCERT, septiembre de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-critica-en-adobe-flash-player-0 (Fecha de consulta, 24/01/2017).

[48] Personal de AndalucíaCERT. <<*Vulnerabilidad crítica en Adobe Flash Player*>>. Web oficial de AndalucíaCERT, octubre de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-critica-en-adobe-flash-player-1 (Fecha de consulta, 24/01/2017).

[49] Equipo de seguridad de Adobe. <<*Adobe. Security Bulletins and Advisories*>>. Web oficial de Adobe. Disponible en línea: https://helpx.adobe.com/security.html (Fecha de consulta, 24/01/2017).

[50] Equipo de seguridad de Oracle. <<*Critical Patch Updates, Security Alerts and Thrid Party Bulletins*>>. Web oficial de Oracle. Disponible en línea: https://www.oracle.com/technetwork/topics/security/alerts-086861.html (Fecha de consulta, 24/01/2017).

[51] Personal de AndalucíaCERT. <<*Vulnerabilidad critica en MySQL*>>. Web oficial de AndalucíaCERT, septiembre de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/alertas-seguridad/vulnerabilidad-critica-en-mysql (Fecha de consulta, 24/01/2017).

[52] Sergio de los Santos. <<*[Webinar 04] Malware en sistemas móviles. Una visión técnica y realista*>>. Formación Cyberseguridad. Seguridad y Confianza Digital. Junta de Andalucía, enero 2017.

[53] Personal de OSI Seguridad. <<*Intentan robarte las credenciales de Bankia utilizando como gancho un SMS*>>. Web oficial de OSI Seguridad, enero de 2016. Disponible en línea: https://www.osi.es/es/actualidad/avisos/2016/01/intentan-robarte-las-credenciales-de-bankia-utilizando-como-gancho-un-sms (Fecha de consulta, 24/01/2017).

[54] Personal de OSI Seguridad. <<*Falsos cupones descuento de Lidl y otras marcas vuelven a la carga*>>. Web oficial de OSI Seguridad, abril de 2016. Disponible en línea: https://www.osi.es/es/actualidad/avisos/2016/04/falsos-cupones-descuento-de-lidl-y-otras-marcas-vuelven-la-carga (Fecha de consulta, 24/01/2017).

[55] Personal de OSI Seguridad. <<*SMS con falsa tarjeta regalo intenta que llames a un 806*>>. Web oficial de OSI Seguridad, junio de 2016. Disponible en línea: https://www.osi.es/es/actualidad/avisos/2016/06/sms-con-falsa-tarjeta-regalo-intenta-que-llames-un-806-0 (Fecha de consulta, 24/01/2017).

[56] Personal de OSI Seguridad. <<*El carro de Navidad gratis que te llega al móvil te puede salir caro, muy caro*>>. Web oficial de OSI Seguridad, diciembre de 2016. Disponible en línea: https://www.osi.es/es/actualidad/avisos/2016/12/el-carro-de-navidad-gratis-que-te-llega-al-movil-te-puede-salir-caro-muy (Fecha de consulta, 24/01/2017).

[57] Personal de OSI Seguridad. <<*Múltiples aplicaciones de Google Play pueden secuestrar tu Android*>>. Web oficial de OSI Seguridad, diciembre de 2016. Disponible en línea: https://www.osi.es/es/actualidad/avisos/2016/12/multiples-aplicaciones-de-google-play-pueden-secuestrar-tu-android (Fecha de consulta, 24/01/2017).

[58] Personal de OSI Seguridad. <<*"Super Mario Run" para Android no existe, todavía*>>. Web oficial de OSI Seguridad, diciembre de 2016. Disponible en línea: https://www.osi.es/es/actualidad/avisos/2016/12/super-mario-run-para-android-no-existe-todavia (Fecha de consulta, 24/01/2016).

[59] Personal de Sophos Iberia. <<*Cuidado con el falso Pokemon GO*>>. Web oficial de Sophos Iberia, julio de 2016. Disponible en línea: http://sophosiberia.es/cuidado-falso-pokemon-go/ (Fecha de consulta, 24/01/2017).

[60] Roman Unuchek. <<*Rooting Pokémons in Google Play Store*>>. SecureList, septiembre de 2016. Disponible en línea: https://securelist.com/blog/mobile/76081/rooting-pokemons-in-google-play-store/ (Fecha de consulta, 18/01/2017).

[61] Equipo de investigadores de CheckPoint. <<*More Than 1 Million Google Accounts Breached by Gooligan*>>. Web oficial de CheckPoint, noviembre de 2016. Disponible en línea:

http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/ (Fecha de consulta, 24/01/2017).

[62] Personal de AndalucíaCERT. <<*Informe de divulgación. El Internet de las cosas (IoT)*>>. Web oficial de AndalucíaCERT, diciembre de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/actualidad/novedades/el-internet-de-las-cosas-iot (Fecha de consulta, 25/01/2017).

[63] Equipo de seguridad de Dyn, Inc. <<*DDoS Attack Against Dyn Managed DNS*>>. Web oficial de Dyn, octubre de 2016. Disponible en línea: https://www.dynstatus.com/incidents/nlr4yrr162t8 (Fecha de consulta, 25/01/2017).

[64] Chema Alonso. <<*Winter is Comming: Algunas reflexiones sobre el DDOS que tumbó Twitter, WhatsApp y alertó al mundo*>>. Un informático en el lado del mal, octubre de 2016. Disponible en línea: http://www.elladodelmal.com/2016/10/winter-is-comming-algunas-reflexiones.html (Fecha de sonculta, 25/01/2017).

[65] Brian Krebs. <<*Hacked Cameras, DVRs Powered Today's Massive Internet Outage*>>. Blog KrebsonSecurity, octubre de 2016. Disponible en línea: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/ (Fecha de consulta, 25/01/2017).

[66] David Bisson. <<*100,000 Bots Infected with Mirai Malware Behind Dyn DDoS Attack*>>. Tripwire. The State of Security, octubre de 2016. Disponible en línea: https://www.tripwire.com/state-of-security/latest-security-news/100000-bots-infected-mirai-malware-caused-dyn-ddos-attack/ (Fecha de consulta, 25/01/2017).

[67] Brian Krebs. <<*KrebsOnSecurity Hit With Record DDoS*>>. Blog KrebsonSecurity, septiembre de 2016. Disponible en línea: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (Fecha de consulta, 25/01/2017).

[68] Editores de Wikipedia. <<*The Shadow Brokers*>>. Wikipedia, la enciclopedia libre. Disponible en línea:https://en.wikipedia.org/wiki/The_Shadow_Brokers (Fecha de consulta, 26/01/2017).

[69] The Shadow Brokers. <<*@shadowbrokerss*>>. Cuenta oficial de Twitter del grupo The Shadow Brokers. Disponible en línea: https://twitter.com/shadowbrokerss?lang=es (Fecha de consulta, 26/01/2017).

[70] Personal de Kaspersky. <<*EQUATION GROUP: QUESTIONS AND ANSWERS*>>. Página web Securelist de Kaspersky, febrero de 2015. Disponible en línea: https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf (Fecha de consulta, 26/01/2017).

[71] Editores de Wikipedia. <<*Fancy Bear*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://en.wikipedia.org/wiki/Fancy_Bear (Fecha de consulta, 26/01/2017).

[72] Editores de Wikipedia. <<*Doping in Russia*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://en.wikipedia.org/wiki/Doping_in_Russia (Fecha de consulta, 27/01/2017).

[73] Redactores de La Vanguardia. <<*EE.UU. expulsa a 35 diplomáticos rusos en respuesta por la injerencia en las elecciones*>>. Diario La Vanguardia, diciembre de 2016. Disponible en línea: http://www.lavanguardia.com/internacional/20161229/412978652503/eeuu-expulsa-diplomaticos-rusos-injerencia-elecciones.html (Fecha de consulta, 27/01/2017).

[74] Manuel Sánchez Gómez-Merelo. <<*La seguridad y las infraestructuras críticas. Sectores estratégicos. Presente y futuro*>>. Web de Tendencias21, febrero de 2016. Disponible en línea: http://www.tendencias21.net/seguridad/La-seguridad-y-las-infraestructuras-criticas-Sectores-estrategicos-Presente-y-futuro_a18.html (Fecha de consulta, 27/01/2017).

[75] Personal del CNPIC. <<*CNPIC. Centro Nacional para la Protección de las Infraestructuras Críticas*>>. Web oficial del CNPIC. Disponible en línea: http://www.cnpic.es/ (Fecha de consulta, 27/01/2017).

[76] E-ISAC (Robert M. Lee, Michael J. Assante & Tim Conway). <<*Analysis of the Cyber Attack on the Ukrainian Power Grid*>>. SANS. Industrial Control Systems, marzo de 2016. Disponible en línea: http://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (Fecha de consulta, 27/01/2017).

[77] Trabajadores de INCIBE. <<*¿Nuevo ciberataque a la red eléctrica de Ucrania?*>>. Web oficial del CERTSI (CERT de Seguridad e Industria), enero de 2017. Disponible en línea: https://www.certsi.es/blog/nuevo-ciberataque-red-electrica-ucrania (Fecha de consulta, 27/01/2017).

[78] Kim Zetter. <<*That Insane, $81M Bangladesh Bank Heist? Here's What We Know*>> Wired, mayo de 2016. Disponible en línea: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/ (Fecha de consulta, 27/01/2017).

[79] Redactores de Muy Computer. <<*Hospital afectado por ransomware paga rescate de 40 bitcoins*>>. Web de Muy Computer, febrero de 2016. Disponible en línea: http://www.muycomputer.com/2016/02/18/hospital-ransomware-rescate-40-bitcoins/ (Fecha de consulta, 27/01/2017).

[80] Redactores de GlobbSecurity. <<*El ransomware vuelve a paralizar un hospital en EEUU*>>. Web de Globb Security, mayo de 2016. Disponible en línea: http://globbsecurity.com/ataque-ransomware-hospital-eeuu-38586/ (Fecha de consulta, 27/01/2017).

[81] José A. González. <<*La epidemia 'ransomware' se expande por los hospitales*>>. Diario Sur, agosto de 2016. Disponible en lína: http://www.diariosur.es/tecnologia/investigacion/201608/07/epidemia-ransomware-expande-hospitales-20160730121821-rc.html (Fecha de consulta, 27/01/2017).

[82] Rene Millman. <<*Nearly 1500 vulnerabilities found in automated medical equipment*>>. SC Magazine UK, marzo de 2016. Disponible en línea: https://www.scmagazineuk.com/nearly-1500-vulnerabilities-found-in-automated-medical-equipment/article/531672/ (Fecha de consulta, 27/01/2017).

[83] Editores de Wikipedia. <<*FBI–Apple encryption dispute*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute (Fecha de consulta, 30/01/2017).

[84] Matt Zapotosky. <<*FBI has accessed San Bernardino shooter's phone without Apple's help*>>. The Washington Post, marzo de 2016. Disponible en línea: https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html?utm_term=.c446ee92cb8e (Fecha de consulta, 30/01/2017).

[85] Redactores de El País. <<*El FBI pagó más de un millón de dólares para desbloquear el iPhone del asesino de San Bernardino*>>. El País, abril de 2016. Disponible en línea: http://internacional.elpais.com/internacional/2016/04/22/actualidad/1461312194_827799.html (Fecha de consulta, 30/01/2017).

[86] Personal de Oficina de Seguridad del Internauta. <<*WhatsApp actualiza sus términos y política de privacidad*>>. Web oficial de la Oficina de Seguridad del Internauta, agosto de 2016. Disponible en línea: https://www.osi.es/es/actualidad/blog/2016/08/30/whatsapp-actualiza-sus-terminos-y-politica-de-privacidad (Fecha de consulta, 30/01/2017).

[87] Redactores de 20 Minutos. <<*Protección de Datos investiga a Whatsapp por compartir números de teléfono con Facebook*>>. Diario online 20 Minutos, octubre de 2016. Disponible en línea: http://www.20minutos.es/noticia/2855850/0/agencia-proteccion-datos-whatsapp-facebook-politica-privacidad/ (Fecha de consulta, 30/01/2017).

[88] Personal de AndalucíaCERT. <<*Informe de divulgación. Predicciones sobre amenazas para 2016*>>. Web oficial de AndalucíaCERT, enero de 2016. Disponible en línea: https://intranet.andcert.junta-andalucia.es/documentacion-tecnica/predicciones-sobre-amenazas-2016 (Fecha de consulta, 30/01/2017).