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

Informe de divulgación

Predicciones de amenazas para el 2017

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-10056-010217*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*01/02/2017*
N° de Páginas	*1 de 16*

1 TABLA DE CONTENIDOS

TABLA DE CONTENIDOS....2
OBJETIVO....3
ALCANCE....3
INTRODUCCIÓN....3
PREDICCIONES DE LAS PRINCIPALES EMPRESAS DEL SECTOR....3
FORTINET....3
MCAFEE....4
KASPERSKY....7
TRENDMICRO....8
CHECKPOINT....9
ESET....10
CONCLUSIONES....12
GLOSARIO....13
DOCUMENTACION DE REFERENCIA....15

2 OBJETIVO

El objeto de este documento es dar a conocer las predicciones de aquellos riesgos y amenazas que acontecerán en el año 2017, basándonos en las tendencias actuales de la ciberdelincuencia. Para ello, se resumirán las predicciones realizadas por algunos de los principales referentes en el mundo de la seguridad.

3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Debe contemplarse como una visión general de aquellos temas que puedan afectarnos a lo largo de este año 2017 en lo que a la ciberseguridad se refiere.

Nos gustaría indicar que este informe no posee una certeza absoluta acerca de sus predicciones, pero puede servir como guía del estado y evolución de los distintos riesgos y amenazas, así como de las medidas a tomar ante éstos.

4 INTRODUCCIÓN

Cada vez existen más dispositivos conectados y se diversifican las tecnologías en uso, por lo que mantener la seguridad de la información constituye un desafío cada vez mayor. En el ecosistema actual coexisten las amenazas más tradicionales (SPAM/Phishing, fugas de información, infecciones por malware, hacktivismo...) con nuevos modelos de cibercrimen (ransomware, APTs, ataques contra infraestructuras críticas, ciberespionaje...)

Ante este panorama, desde AndalucíaCERT hemos considerado oportuno elaborar el presente informe divulgativo para que el lector pueda hacerse una idea de lo que deparará el año 2017 en cuanto a ciberseguridad.

5 PREDICCIONES DE LAS PRINCIPALES EMPRESAS DEL SECTOR

En este epígrafe se resumirán las principales predicciones acerca de los riesgos y amenazas que tendrán lugar este año 2017. Para ello nos basaremos en los informes elaborados por algunas de las principales empresas del sector.

5.1 FORTINET

1. *El malware se hará más inteligente y autónomo*

   Según Fortinet, en los próximos años nacerá una nueva generación de malware que será capaz de operar de forma autónoma. Aprenderá a conocer la situación y el ambiente en el que se encuentra para poder tomar decisiones y actuar de forma más "humana". En otras palabras, el malware se hará "inteligente" para optimizar el ataque.

2. *Los fabricantes de IoT tendrán que rendir cuentas por la seguridad de sus productos*

   Los dispositivos del Internet de las Cosas (IoT) serán uno de los objetivos preferidos de los ciberdelincuentes, por lo que aumentará la preocupación de los consumidores, proveedores y gobiernos para que se cumplan ciertos estándares de seguridad.

3. *Uso de dispositivos IoT comprometidos para realizar ataques*

   Siguiendo con la tendencia iniciada en 2016, los ciberdelincuentes comprometerán dispositivos IoT para usarlos en ataques posteriores, especialmente contra infraestructuras en la nube.

4. *Los cibercriminales empezarán a atacar las ciudades inteligentes*

   Debido al auge de esta tecnología emergente, los ciberdelincuentes comenzarán a realizar ataques contra *smart cities*. Se esperan apagones en sistemas de alumbrado público, edificios inteligentes o semáforos para pedir un rescate a cambio de que todo vuelva a la normalidad.

5. *El ransomware se profesionaliza*

   El modelo de negocio conocido como RaaS (*Ransomware as a Service*) se establecerá como uno de los más lucrativos para los cibercriminales, permitiendo a personas sin conocimientos técnicos propagar este tipo de malware. Además, se espera que los ataques por ransomware comiencen a ser cada vez más dirigidos, buscando objetivos que proporcionen una mayor recompensa económica.

6. *Escasez de talento en el campo de la ciberseguridad*

   Fortinet se hace eco de algunas de las noticias publicadas en los últimos tiempos que hablan de la dificultad que encuentran las empresas para localizar perfiles específicos en ciberseguridad. Este hecho generará problemas, dado que ciertos puestos se quedarán sin cubrir.

5.2 MCAFEE

1. *El ransomware remitirá en la segunda mitad de 2017*

   La firma McAfee augura que el ransomware seguirá considerándose una amenaza relevante hasta la segunda mitad de 2017, momento en el que remitirá. Para realizar esta afirmación, la compañía propiedad de Intel se basa en el hecho de que cada vez surgen más proyectos similares a No More Ransom! y herramientas como AntiRansom o LatchARW. Estas iniciativas ayudarán a poner freno a la expansión del ransomware, pero no lo eliminarán por completo.

2. *Los ataques que aprovechan vulnerabilidades de Windows disminuyen mientras los casos aumentan en otras plataformas*

   Las nuevas medidas de seguridad implementadas en los sistemas operativos de Microsoft han complicado la elaboración de exploits, por lo que McAfee pronostica un aumento en el desarrollo de exploits para otras plataformas: los intentos de explotación para productos como Flash y Java se seguirán produciendo (aunque se espera que en menor medida). De igual forma, se producirá un

aumento del malware de tipo macro en documentos ofimáticos, así como exploits para aplicaciones con código heredado que no ha sido convenientemente auditado.

3. *El hardware y el firmware, objetivos cada vez más habituales de ciberdelincuentes sofisticados*

   El firmware, es decir, el microcontrolador y la pila de software del que disponen los sistemas informáticos para realizar pequeñas tareas de mantenimiento e inicialización, tiene propiedades que lo convierten en un objetivo atractivo para los ciberdelincuentes: se almacena en un espacio no volátil, tiene acceso completo al hardware que gestiona y está bastante oculto de los sistemas operativos y del software de seguridad. No es un objetivo fácil, pero cuando el ataque funciona ofrece máxima persistencia, amplias posibilidades de pasar desapercibido, acceso a gran variedad de recursos y una vía para implantar puertas traseras en el equipo.

   Según McAfee, se prevé que para el 2017 los ataques se harán más sofisticados para poder encontrar vulnerabilidades en el hardware y en el firmware. Se atacarán sistemas como la BIOS y el UEFI instalando en ellos malware de tipo bootkit.

4. *El secuestro de drones pone la amenaza en el cielo*

   Lo que comenzó siendo un juguete se ha convertido en una herramienta de trabajo para ciertos sectores: paquetería, fotógrafos, agricultores, fuerzas y cuerpos de seguridad... No obstante, la seguridad de estos aparatos es bastante cuestionable, por lo que se prevé que en 2017 se den bastantes casos de drones secuestrados o derribados electrónicamente. En este sentido, sería lógico que las leyes evolucionen para regir cuándo y dónde se pueden volar los drones, así como para exigir unos estándares de seguridad a los fabricantes de éstos.

5. *Las amenazas a dispositivos móviles incluirán el ransomware, las herramientas de acceso remoto y los mercados de apps comprometidas*

   McAfee prevé que el malware para móviles siga creciendo en 2017, con ransomware, troyanos bancarios y herramientas de acceso remoto entre las principales amenazas. Por este motivo se recomienda descargar apps únicamente desde markets oficiales y de confianza, así como revisar la reputación del autor de la app y los permisos que solicita antes de instalarla.

6. *El malware para el Internet de las cosas abre una puerta trasera a los hogares*

   La electrónica de consumo sigue creciendo con rapidez, destacando especialmente los dispositivos IoT. Por este motivo la carrera por salir al mercado es feroz y los fabricantes suelen dejar en un segundo plano la seguridad de sus productos. Este hecho provoca que el IoT se haya convertido en uno de los objetivos predilectos de los ciberdelincuentes. De hecho, se espera que en 2017 comiencen a aparecer casos de código malicioso preinstalado en algunos dispositivos IoT, puesto que se comprometerán algunas librerías frecuentemente usadas por los fabricantes.

7. *El aprendizaje automático acelera los ataques de ingeniería social*

   El aprendizaje automático consiste en la rama de la inteligencia artificial que desarrolla técnicas que permiten a las computadoras "aprender", creando programas que generalicen comportamientos a partir de una información suministrada en forma de ejemplos.

   Los ciberdelincuentes también están incluyendo estas técnicas en sus ataques, por lo que se prevé que en 2017 sean cada vez más sofisticados y dañinos.

8. *La explosión de anuncios falsos y "Me gusta" comprados erosiona la confianza*

   Dentro de los esquemas de tipo *clickfraud* se observará un aumento en el uso de "reputaciones compradas". En otras palabras, los ciberdelincuentes comprarán buenas referencias en las redes sociales para páginas o productos fraudulentos, haciéndolos parecer más creíbles y legítimos. De igual forma, se espera un aumento en el número de advertencias de seguridad falsas, como los tradicionales *FakeAV*.

9. *La escalada de la guerra de anuncios potencia la distribución de malware*

   En 2017 los creadores de malware se servirán de las técnicas que usan los anunciantes para eludir los bloqueadores de contenido y así permitir la descarga camuflada de código dañino a través de la publicidad que, en muchos casos, estará incrustada en webs legítimas.

10. *Los hacktivistas divulgan problemas de privacidad*

    Los hacktivistas van a lanzar ataques e infiltrarse en diversas empresas y organizaciones para obtener datos de usuarios, hacerlos publico y forzar a que se adopten medidas para evitar casos similares en un futuro.

11. *Las operaciones de desmantelamiento de las fuerzas de seguridad golpean a la ciberdelincuencia*

    En 2017 la cooperación entre el sector privado y las fuerzas de seguridad se hará mucho más presente. Por tanto, aumentará el número de operaciones en las que se desmantelarán infraestructuras criminales de distribución de malware, alquiler de botnets, envío de SPAM/Phishing...

12. *El intercambio de inteligencia sobre amenazas hace grandes progresos*

    En 2017, las principales organizaciones y empresas del sector crearán iniciativas para intercambiar información sobre amenazas, por lo que resultará más fácil identificarlas y combatirlas.

13. *Ciberespionaje: la industria y las fuerzas de seguridad aúnan esfuerzos*

    Continuando con la tendencia de los últimos años, el 2017 nos deparará nuevos ejemplos de ciberespionaje y ciberguerra. Además, como sucedió con Equation Group, se filtrarán nuevos exploits y ataques usados por entes patrocinados por agencias gubernamentales.

14. *Los sectores de la seguridad física y la ciberseguridad colaboran estrechamente*

    Según McAfee, los sectores de la seguridad física y la ciberseguridad trabajarán conjuntamente para crear soluciones de seguridad, de forma que un único proveedor sea el encargado de ofrecer todo tipo de soluciones de seguridad a sus clientes.

5.3 KASPERSKY

1. *Esas temidas APTs*

   Para Kaspersky, los ataques llevados a cabo mediante el uso de APTs continuarán produciéndose, pero veremos algunas novedades: se producirá un incremento de los "implantes pasivos", es decir, malware que una vez infectado el equipo permanece inactivo (a veces durante años) hasta que un determinado patrón provoca que se inicien sus actividades maliciosas; se observarán cada vez más "infecciones efímeras", es decir, malware residente en la memoria RAM y, por tanto, volátil; aumentarán las campañas de espionaje en dispositivos móviles, puesto que los sistemas de escritorio quedan cada vez más en un segundo plano.

2. *El futuro de los ataques financieros*

   Aumentará el interés de los ciberdelincuentes por los ataques financieros, especialmente contra la red SWIFT y las plataformas de sistemas de pago.

3. *El ransomware deshonesto*

   Se prevé un aumento del tipo de ransomware denominado "*skiddie*" (escrito o adaptado por novatos), lo cual provocará que aunque se haga efectivo el pago del rescate, realmente no se podrán recuperar los datos secuestrados debido a la falta de profesionalidad de los cibercriminales.

4. *Ataques a infraestructuras industriales*

   Continuarán produciéndose incidentes como el de Stuxnet, lo cual provocará un miedo generalizado a los accidentes de cibersabotaje industrial y forzará al sector a tomar medidas.

5. *Un Internet superpoblado*

   La débil seguridad del Internet de las Cosas (IoT) continuará generando incidentes de seguridad, principalmente mediante la realización de ataques tipo DDoS usando botnets compuestas por estos dispositivos. De igual forma, continuarán apareciendo exploits y zero-days en equipamiento de red (routers, switches, firewalls, appliances...).

6. *La guerra de la información*

   Los ataques cibernéticos cobran cada vez más importancia en las relaciones internacionales. Y es que la ciberseguridad supone un nuevo desafío para la comunidad internacional y la relaciones políticas

entre países. Las ciberamenazas podrían, potencialmente, poner en peligro los intereses y la economía de un estado.

En este 2017 los ataques orquestados por entes gubernamentales continuarán, e incluso se prevé que se produzcan operaciones de bandera falsa, es decir, operaciones encubiertas diseñadas para parecer como si fueran llevadas a cabo por otras entidades.

7. *Hacktivismo*

Los métodos cada vez más intrusivos usados por la industria: el rastreo de usuarios mediante el uso de *supercookies* y la creación de perfiles de usuarios en base a su huella digital, el tratamiento de los datos personales por parte de algunas corporaciones, etc. potenciará el fenómeno del hacktivismo. Los activistas llevarán a cabo ataques cibernéticos y posteriormente realizarán filtraciones de información buscando eco mediático y dañar la imagen pública de ciertas entidades.

5.4 TRENDMICRO

1. *El crecimiento de ransomware se estabilizará en 2017*

Trendmicro predice un crecimiento del 25% en el número de nuevas familias de ransomware en 2017 (unas 15 nuevas familias cada mes). Sin embargo, los ciberdelincuentes tendrán que diversificarse y atacar otros objetivos y plataformas. Además, comenzaremos a ver cómo primero se robarán los datos confidenciales para venderlos en el mercado negro y luego se instalará ransomware en los servidores para así incrementar las ganancias.

Por otro lado, el ransomware contra los entornos industriales y los ataques a los dispositivos del IoT también verán incrementado su número.

2. *Los dispositivos IoT jugarán un papel más importante en los ataques DDoS y se incrementarán los ataques contra el IIoT (el Internet Industrial de las Cosas)*

Se prevé que los ciberdelincuentes usarán malware parecido a Mirai para infectar dispositivos IoT y realizar ataques tipo DDoS como el sufrido el pasado año 2016 por la empresa DynDNS.

Por otro lado, la enorme cantidad de vulnerabilidades que están apareciendo en diversos sistemas de control industrial, así como el auge del denominado IIoT (Internet Industrial de las Cosas) provocará una oleada de ataques contra estos sistemas.

3. *El Compromiso del Correo Electrónico Corporativo*

El compromiso de las cuentas corporativas como forma rentable de acceder a la información confidencial de las empresas continuará creciendo, ya que se trata de ataques relativamente sencillos de realizar y que han demostrado ser muy lucrativos para los ciberdelincuentes.

4. *El Compromiso de los Procesos de Negocio*

   Esta categoría de ataque requiere un conocimiento exhaustivo de los procesos de negocios de la organización que se elija como víctima. Los hackers se infiltran en la empresa y agregan, modifican, eliminan o interceptan entradas y transacciones con el objetivo final de recibir un pago no autorizado a una cuenta bancaria que ellos mismos controlan.

5. *Adobe y Apple superarán a Microsoft en cuanto a vulnerabilidades descubiertas*

   Para TrendMicro, este 2017 se descubrirán más defectos de software en productos de las compañías Adobe y Apple, llegando a superar los que se hallen en el software de Microsoft. Obviamente, una vez descubiertas dichas vulnerabilidades, serán añadidas a los diferentes kits de exploits usados por los delincuentes.

6. *La ciberpropaganda se convertirá en una norma*

   Con la mitad de la población mundial conectada a Internet, el aumento de la ciberpropaganda continuará, y se convertirá en una herramienta muy útil para influir en la opinión pública. En 2017 se verá mucho más uso y abuso de las redes sociales con estos fines.

7. *Aplicación y cumplimiento de la normativa general de protección de datos*

   La aplicación y cumplimiento de la GDPR (Ley Europea de Protección de Datos) forzará cambios políticos y administrativos, lo cual impactará en los costes, debido a que las organizaciones han de llevar a cabo revisiones completas en sus sistemas para asegurar dicho cumplimiento. De igual forma, un DPO (Delegado de Protección de Datos) será una figura obligatoria en las organizaciones.

8. *Nuevos actores en el panorama internacional y nuevos métodos de ataques dirigidos*

   Aparecerán nuevas tácticas de ataque dirigidas que se centrarán en eludir las modernas técnicas de detección, y esto permitirá a los ciberdelincuentes volverse más experimentados y llegar incluso a realizar ataques contra gobiernos.

5.5 CHECKPOINT

1. *El ecosistema móvil*

   El incremento en el uso de smartphones y tablets, unido al cada vez más extendido BYOD, hará que crezcan los ataques contra estos dispositivos. Según Check Point, en 2017 uno de cada cinco empleados será responsable de alguna brecha de seguridad que afecte a datos corporativos debido a algún tipo de infección por malware en su terminal móvil.

2. *Internet de las cosas (IoT) e Internet Industrial de las Cosas (IIoT)*

   Es un hecho que aún existen muchos fabricantes que no han tenido en cuenta la seguridad en el diseño e implementación de sus dispositivos inteligentes. Por este motivo, se espera un crecimiento de los ataques contra el IoT y el IoT Industrial, especialmente contra los sistemas SCADA.

3. *Infraestructuras críticas*

   Hay que tener en cuenta que muchas infraestructuras críticas fueron diseñadas en su momento sin tener en cuenta la seguridad, por lo que son un blanco fácil. Según Check Point, los responsables de seguridad de estos sistemas tienen que prestar especial atención a tres frentes potenciales de ataque: otros países, terrorismo y crimen organizado.

4. *Prevención de amenazas: ransomware*

   En 2017 el ransomware será tan común como los ataques DDoS, por lo que las empresas deberán estar preparadas, tendrán que usar técnicas de sandboxing avanzado y de prevención de amenazas, para así proteger sus redes de un modo efectivo ante estos secuestros.

5. *La nube*

   La compañías seguirán almacenando sus datos en la nube, por lo que los proveedores de estas infraestructuras se convertirán en objetivo prioritario de los cibercriminales, ya que un ataque exitoso no sólo afectará al proveedor, sino a todos sus clientes. Además, crecerán los ataques de ransomware que afecten a centros de datos alojados en la nube.

5.6 ESET

1. *RoT: el ransomware de las cosas*

   ESET nos avanza que en 2017 aparecerán casos de secuestro digital de dispositivos conectados, como coches y neveras inteligentes, manteniendo el dispositivo bloqueado hasta que se pague un rescate. En definitiva, el ransomware del Internet de las Cosas.

2. *La educación en seguridad, una responsabilidad a nivel social*

   Aunque es cierto que existen técnicas de explotación cada vez más complejas, la realidad demuestra que los ataques más efectivos suelen involucrar técnicas de ingeniería social. Debido al desconocimiento de los usuarios, el engaño suele resultar el método más sencillo para atacar un sistema.

   Es importante que en este año se tienda a concienciar e informar a los usuarios. Es importante que conozcan las amenazas y sus consecuencias, así como unas mínimas pautas de detección y prevención. Para ello será indispensable la participación activa de gobiernos y empresas.

3. *Ecosistema móvil: el malware y su realidad... ¿aumentada?*

   El mercado de apps para terminales móviles no deja de crecer y hacerse cada vez más complejo. Un claro ejemplo es el auge de las tecnologías de realidad aumentada. Ante este escenario, los usuarios deberán prestar atención a las aplicaciones que instalan en sus terminales y evitar descargar malware que intente hacerse pasar por alguna app oficial.

   Por otro lado, los diseñadores no sólo tendrán que tener en cuenta la protección de datos, sino también el diseño de un modelo de seguridad inherente a la creación de nuevas aplicaciones.

   Según ESET, durante 2017 se observará más ransomware para móviles, más apps falsas, códigos maliciosos más complejos y muchas más estafas a través de WhatsApp y redes sociales.

4. *Vulnerabilidades:los reportes bajan, pero ¿estamos más seguros?*

   Pese a que la tecnología sigue avanzando de forma imparable, la cantidad de vulnerabilidades reportadas en los últimos tiempos se mantiene más o menos constante. Esto se debe en parte a los nuevos modelos en el desarrollo de sistemas, en la que se comienza a priorizar la seguridad de la información.

   El reto para el 2017 consiste en mejorar la gestión de las vulnerabilidades que se vayan descubriendo, enfocándola para lograr una adecuada implementación de políticas de seguridad y planes de continuidad de negocio, e incluyendo una comunicación de los incidentes para mantener informados a los usuarios. Por otro lado, respecto a los desarrolladores, se espera que se continúe afianzando el paradigma del desarrollo seguro.

5. *Software de seguridad de nueva generación: mitos y marketing*

   Últimamente están apareciendo nuevas tecnologías de detección de malware, llamadas de nueva generación, que no se basan en la detección mediante el uso de firmas, sino que usan aprendizaje automático, análisis del comportamiento...

   Según ESET, en 2017 estas nuevas tecnologías deberán usarse en combinación con las técnicas tradicionales (basadas en el uso de firmas) para lograr que las empresas y los particulares se beneficien de ellas y aprovechen todo su potencial.

6. IoT *y ransomware en el sector de la salud: la punta del iceberg*

   ¿Qué podría ser más importante que proteger los sistemas de la industria de la salud? Los centros de salud y los hospitales suponen un objetivo particularmente atractivo para los ciberdelincuentes, por lo que el sector sanitario se seguirá enfrentando a desafíos importantes en cuanto a la seguridad en 2017.

El ransomware en centros sanitarios se convertirá en algo común durante 2017, puesto que los ciberdelincuentes han comprendido que los datos médicos son mucho más importantes y pueden incluso suponer una cuestión de vida o muerte, lo cual forzaría a estas instituciones a pagar el rescate para recuperar los datos de sus pacientes. Además, la introducción de dispositivos, aparatos e instrumental médico conectado, siguiendo los principios del IoT, aumentará la superficie de exposición y, por tanto, hará que estas entidades sean más fáciles de atacar.

7. *Amenazas para infraestructuras críticas: la dimensión de Internet*

   ESET, al igual que el resto de empresas del sector, cree que los ataques cibernéticos contra las infraestructuras críticas continuarán siendo tendencia en 2017, con sus consecuentes efectos negativos y el peligro que puede suponer para toda la población.

8. *Desafíos e implicaciones de legislaciones sobre ciberseguridad*

   Ante el complejo escenario en el que nos encontramos, queda patente la necesidad de un marco normativo sobre ciberseguridad que sea de aplicación a gran escala. El propósito es que las legislaciones de los distintos países comiencen a considerar las medidas y elementos necesarios para la seguridad, empezando por la respuesta a incidentes de gran escala, la protección de infraestructuras críticas, la colaboración entre organismos y la concienciación de los usuarios. Se prevé que en 2017 se realicen algunos avances en este sentido.

9. *Plataformas de juego: los riesgos potenciales de consolas integradas a computadoras*

   Se prevé que la industria de los videojuegos continúe expandiéndose y, por tanto, generando un volumen de negocio de proporciones titánicas, por lo que será uno de los objetivos de los ciberdelincuentes.

   Las amenazas se irán adaptando a los cambios en el modo en que se distribuyan y desarrollen los juegos. Además, muchas de las principales plataformas presentan ciertos aspectos muy deseables para los cibercriminales: tienen acceso a datos personales y números de tarjetas de crédito. Es por ello que los desarrolladores de juegos deberán comenzar a considerar la seguridad de sus clientes.

6 CONCLUSIONES

Como el lector habrá podido comprobar, la mayoría de las empresas del sector coinciden en los siguientes puntos:

- El ransomware se convierte en pandemia y diversifica sus objetivos.
- La escasa seguridad de los dispositivos IoT nos traerá más de un quebradero de cabeza.
- Los ataques contra sistemas industriales e infraestructuras críticas aumentarán.
- Vivimos en un escenario de ciberguerra encubierta y espionaje en la red.

7 GLOSARIO

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.

BIOS: Siglas de la expresión inglesa *Basic Input Output System*. Firmware instalado en un ordenador personal. Se trata del primer programa que se ejecuta cuando se enciende.

bootkit: Conjunto de herramientas de explotación de sistemas que operan en el momento del arranque.

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

BYOD: Siglas de la expresión inglesa *Bring Your Own Device*. Política empresarial que favorece que los empleados lleven sus propios dispositivos al lugar de trabajo.

clickfraud: Fraude que tiene lugar en Internet y que consiste en generar ganancias por anuncios de publicidad del tipo *pay-per-click*. En la mayoría de las ocasiones, los clicks en dichos anuncios son realizados de forma automática por códigos maliciosos, aunque también puede haber interacción del usuario.

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

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.

DPO: Siglas de la expresión inglesa *Data Protection Officer* (en español, Delegado de Protección de Datos). Figura obligatoria que aparece en la regulación europea sobre Protección de Datos (GDPR).

drone: Vehículo aéreo no tripulado. Se trata de una aeronave que vuela sin tripulación, de manera autónoma o controlado remotamente.

FakeAV: Falso antivirus. Tipo de malware que trata de hacerse pasar por un software antivirus legítimo.

firmware: Programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

GDPR: Siglas de la expresión inglesa *General Data Protection Regulation*. Regulación europea sobre Protección de Datos.

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

IIoT: Siglas de la expresión inglesa *Industrial Internet of Things*. Igual que el Internet de las cosas, pero orientado al mundo industrial.

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 y el engaño 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...

RaaS: Siglas de la expresión inglesa *Ransomware as a Service*. Modelo de negocio ofrecido por los cibercriminales en el que se profesionaliza la creación de malware de tipo ransomware.

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

RoT: Siglas de la expresión inglesa *Ransomware of Things*. Hace referencia al malware de tipo ransomware específicamente orientado a dispositivos del Internet de las Cosas.

sandboxing: Técnica que implica la ejecución de software en un entorno aislado y controlado, generalmente una máquina virtual.

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.

smart cities: En español, ciudades inteligentes. Se refiere a un tipo de desarrollo urbano basado en la sostenibilidad, que hace uso de las Tecnologías de la Información para controlar ciertos aspectos como el alumbrado público.

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.

UEFI: Siglas de la expresión *Unified Extensible Firmware Interface*. Sistema que reemplaza a la BIOS en los sistemas modernos.

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

8 DOCUMENTACION DE REFERENCIA

[1] Derek Manky. <<*Fortinet 2017 Cybersecurity Predictions: Accountability Takes the Stage*>>. Fortinet Blog, noviembre de 2016. Disponible en línea: https://blog.fortinet.com/2016/11/21/fortinet-2017-cybersecurity-predictions-accountability-takes-the-stage

[2] Christiaan Beek, Yuriy Bulygin, Douglas Frosst & Otros. <<*McAfee Labs. Predicciones sobre amenazas para 2017*>>. McAfee Labs Reports, noviembre de 2016. Disponible en línea: https://www.mcafee.com/es/resources/reports/rp-threats-predictions-2017.pdf

[3] Costin Raiu, Juan Andrés Guerrero-Saade y el personal de Kaspersky Labs. <<*Predictions for 2017: "Indicators of compromise" are dead*>>. Kaspersky Security Bulletin, noviembre de 2016. Disponible en línea: https://kasperskycontenthub.com/securelist/files/2016/11/KL_Predictions_2017.pdf

[4] Personal de TrendMicro. <<*The Next Tier – Trend Micro Security Predictions for 2017*>>. Web oficial de TrendMicro, diciembre de 2016. Disponible en línea: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-next-tier.pdf

[5] Equipo de Investigación de Check Point. <<*Check Point's Cyber Security Predictions for 2017*>>. Blog de Check Point, octubre de 2016. Disponible en línea: http://blog.checkpoint.com/2016/10/25/check-points-cyber-security-predictions-2017/

[6] Personal de ESET. <<*La seguridad como rehén. Tendencias 2017*>>. We live Security, diciembre de 2016. Disponible en línea: http://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf

[7] Personal de S21Sec. <<*Informe de predicciones para el 2017*>>. Web oficial de S21Sec, año 2016. Disponible en línea: http://www.economiadehoy.es/adjuntos/11948/S21sec_InformePredicciones_2017.pdf