sedian

Seguridad Digital
de Andalucía

Informe

Predicciones de amenazas para el 2018

Tipo de documento: Informe

Autor del documento: AndalucíaCERT

Código del documento: CERT-IF-20180603-00

Edición: 0

Categoría: Público

Fecha de elaboración: 06/03/2018

JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

ÍNDICE

1 Objeto

El objeto de este documento es dar a conocer las predicciones de aquellos riesgos y amenazas que acontecerán en el año 2018, en base a las tendencias actuales de ciberdelincuencia. Para ello, se resumirán las predicciones realizadas por algunos de los principales referentes en el mundo de la seguridad.

2 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 afectar a lo largo de este año 2018 en lo que a la ciberseguridad se refiere.

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 estos.

3 Introducción

Cada vez existen más dispositivos conectados y se diversifican más 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 se ha considerado oportuno elaborar el presente informe divulgativo para que el lector pueda hacerse una idea de lo que deparará el año 2018 en cuanto a lo que en ciberseguridad se refiere.

4 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 2018 según los informes elaborados por algunas de las principales empresas del sector.

4.1 Fortinet

- La extorsión de los servicios comerciales es un gran negocio.

Los próximos grandes objetivos del ransomware serán probablemente los proveedores de servicios en la nube y otros servicios comerciales con el objetivo de crear flujos de ingresos. Las complejas redes que han desarrollado los proveedores en la nube pueden producir un punto único de fallo para cientos de empresas, entidades gubernamentales,

infraestructuras críticas y organizaciones. El impacto de tales ataques podría ocasionar un pago masivo e interrumpir el servicio para numerosas empresas y clientes.

- Infraestructura crítica a la vanguardia.

La mayoría de las redes de infraestructura operacional y de infraestructura crítica son notoriamente frágiles ya que originalmente fueron diseñadas para ser aisladas. La expectativa por responder a la demanda de los empleados y consumidores ha comenzado a cambiar los requisitos de estas redes, impulsando la necesidad de seguridad avanzada. Dada la importancia de estas redes y los potenciales resultados devastadores si se viesen comprometidas o desconectadas, los proveedores de infraestructura crítica se encuentran ahora en una carrera contra organizaciones criminales, terroristas y de estado para asegurar dichas infraestructuras.

- Aumento de hivenets y swarmbots con autoaprendizaje.

Los ciberdelincuentes reemplazarán las botnets por grupos inteligentes de dispositivos comprometidos llamados hivenets para crear vectores de ataque más efectivos. Los hivenets aprovecharán el autoaprendizaje para enfocarse en sistemas vulnerables a una escala sin precedentes. Serán capaces de comunicarse entre ellos y tomar medidas basadas en la inteligencia compartida, pudiendo llegar a actuar sin que el líder de botnets les ordene que lo hagan. Como resultado, podrán crecer exponencialmente como enjambres, ampliando la capacidad de atacar

simultáneamente a múltiples víctimas impidiendo significativamente la mitigación y la respuesta. Estos enjambres de dispositivos comprometidos o swarmbots se podrán utilizar para identificar y atacar diferentes objetivos a la vez.

- La deep web y la economía del cibercrimen ofrecerán nuevos servicios basados en la automatización.

Se esperan nuevas ofertas de servicios desde la deep web, ya que organizaciones basadas en el crimen como servicio (CaaS) usarán nuevos conceptos tecnológicos como el aprendizaje automatizado, para modificar el código sobre la marcha en función de cómo y qué se ha detectado a fin de que estas herramientas de penetración sean más indetectables.

- Malware polimórfico de próxima generación.

Pronto se comenzará a ver el malware completamente creado por máquinas, basado en detección automatizada de vulnerabilidades y análisis de datos complejos. Actualmente ya se pueden usar modelos de aprendizaje para evadir la seguridad y producir más de un millón de variaciones de virus en un día. El malware polimórfico no es nuevo, pero está a punto de adquirir una nueva cara aprovechando la IA para crear código sofisticado que pueda aprender a evadir la detección a través de rutinas.

4.2 McAfee

- Carrera armamentística en torno al machine learning.

Para ganar esta "carrera armamentista" que se disputa contra los cibercriminales, las organizaciones deberán aumentar la "inteligencia" de las máquinas y la velocidad de las respuestas orquestadas junto a la capacidad estratégica de las personas. De esta forma, las organizaciones podrán comprender y anticiparse a los patrones de desarrollo de ataques, incluso si estos no se han producido con anterioridad.

- El ransomware evolucionará de la extorsión tradicional a nuevas tecnologías y objetivos.

La rentabilidad de las campañas tradicionales de ransomware seguirá disminuyendo a medida que las defensas de los fabricantes, la educación de los usuarios y las estrategias de la industria mejoren. Los atacantes centrarán sus ataques de ransomware en objetivos menos tradicionales y más rentables, que incluyen individuos de alto poder adquisitivo, dispositivos conectados y negocios o servicios con gran cantidad de usuarios.

- Las aplicaciones serverless ahorrarán tiempo y reducirán los costes, pero también aumentarán las superficies de ataque para las organizaciones que las implementan.

Estas aplicaciones, que permiten un mayor grado de granularidad de los servicios, también son vulnerables a los ataques contra los datos en

tránsito en la red y potencialmente, a ataques de denegación de servicio, en los que dada la arquitectura de estas aplicaciones, se traduce en costosas interrupciones del servicio prestado.

- Los fabricantes de dispositivos conectados para el hogar y los proveedores de servicios buscarán superar los reducidos márgenes de beneficio a través de la recopilación de nuestros datos, con o sin nuestro consentimiento.

Teniendo en cuenta que los usuarios rara vez leen los acuerdos de privacidad, las empresas se verán tentadas a cambiarlos para obtener más información, además, habrá consecuencias legales para aquellas compañías que estén pensando en romper las reglas, pagar las respectivas multas y luego continuar con estas prácticas.

- Las organizaciones que recogen contenido digital creado por los más jóvenes podrán ver comprometida su reputación a largo plazo.

Las empresas se volverán más agresivas al permitir y recopilar contenido generado por los usuarios más jóvenes. En 2018, los padres se darán cuenta de los abusos corporativos del contenido digital generado por los menores y tendrán más en cuenta las posibles implicaciones a largo plazo de este tipo de prácticas para sus hijos.

4.3 Kaspersky

- Más ataques a la cadena de suministro.

Durante 2018 se espera ver más ataques a la cadena de suministro, tanto reales como detectados. El uso de programas especializados infectados con troyanos en regiones y sectores específicos se convertirá en un movimiento similar al de los ataques waterholing dirigidos a sitios y víctimas específicas.

- Más malware de alta gama en móviles.

La cantidad total de malware móvil que existe en el mundo real puede ser mayor a la que se tiene registrada. Esto se debe a deficiencias en la detección y erradicación. Se estima que en 2018 se descubrirá más malware para móviles como resultado tanto del aumento en los ataques, como de la mejora en las tecnologías de seguridad diseñadas para detectarlos.

- Ataques sofisticados UEFI y BIOS.

Se sabe que existe malware UEFI de grado comercial desde 2015, con eso en mente, es sorprendente que no se haya encontrado malware UEFI significativo, un hecho que se atribuye a la dificultad para detectarlo. Se estima que en 2018 se descubrirá más malware basado en UEFI y BIOS.

- Más subversión de criptografía.

Ante la gran cantidad de las tecnologías de cifrado que se utilizan en nuestra vida cotidiana: desde tarjetas inteligentes y redes inalámbricas hasta tráfico web cifrado. En 2018, se anticipa que se encontrarán

vulnerabilidades criptográficas más severas y serán parcheadas, ya sea en los estándares mismos o en implementaciones específicas.

- La identidad en el comercio electrónico entrará en crisis.

Los datos fundamentales de identificación están tan expandidos que ya no son confiables en absoluto. El comercio y las instituciones gubernamentales tendrán que elegir entre reducir la comodidad de realizar operaciones importantes por Internet o duplicar la adopción de otras soluciones. Tal vez alternativas como el pago móvil se pondrán de moda como forma de asegurar la identidad y las transacciones pero, mientras tanto, es posible que veamos una ralentización en el rol crítico de Internet para modernizar procesos burocráticos tediosos y recortar los costes operativos.

- Más ataques a módems y routers.

Debido a que estos equipos cuentan con acceso constante a Internet, se convierten en un blanco codiciado para los atacantes que quieren tener un acceso persistente y sigiloso a la red. Además, en algunos casos los atacantes pueden hacerse pasar por usuarios de Internet para desviar el camino de un atacante por completo hacia una dirección de conexión diferente y así suplantar la identidad de otros con distintos fines.

- Un medio para el caos social.

Las redes sociales (que basan su éxito en métricas cuantificadas como usuarios activos diariamente) tienen muy poco incentivo para purgar

los bots de sus usuarios. Se espera que a medida de que este tipo de abuso continúe y las grandes redes de bots sigan siendo explotadas, las redes sociales sufran la mayor repercusión por parte de los usuarios, que molestos con estos hechos, buscarán alternativas para reemplazar este tipo de redes.

4.4 Trend Micro

- El modelo de negocio de ransomware seguirá siendo un pilar de la ciberdelincuencia

Con el ransomware como servicio (RaaS) que aún se ofrece en foros clandestinos, junto con el bitcoin como método seguro para cobrar rescate, los ciberdelincuentes se sienten cada vez más atraídos por este "modelo comercial". Los atacantes seguirán confiando en las campañas de suplantación de identidad (phishing) donde los correos electrónicos con la carga de ransomware se entregan en masa para garantizar un mayor porcentaje de usuarios afectados. También optarán por una inversión mayor al apuntar a una sola organización, posiblemente en un entorno de Internet industrial de las cosas (IIoT), como un ataque de ransomware que interrumpiría las operaciones y afectaría a la línea de producción.

- Los ciberdelincuentes explorarán nuevas formas de abusar de los dispositivos de IoT para su propio beneficio.

Se prevé que además de realizar ataques DDoS, los ciberdelincuentes recurrirán a dispositivos IoT para hacer de proxy y que confundan tanto su

ubicación como el tráfico web, teniendo en cuenta que las fuerzas del orden suelen referirse a direcciones IPs y registros para la investigación criminal y los análisis forenses posteriores a la infección.

- Las pérdidas globales de las estafas de compromiso de email empresarial superarán los 9 mil millones de dólares en 2018.

Se continuarán viendo estafas de BEC que involucran a ejecutivos de compañías que son suplantados para transferir sumas de dinero. Se ha observado un aumento de los intentos de ataque de BEC que involucran fraude de CEO. También es interesante observar que, en lugar de implantar keyloggers, los estafadores de BEC recurren a los sitios y a PDFs de phishing, que son más baratos que los registradores de pulsaciones de teclas.

- Las campañas de ciberpropaganda se perfeccionarán utilizando técnicas probadas de campañas pasadas de SPAM.

Las noticias falsas y la ciberpropaganda continuarán porque no ha habido una manera confiable de detectar o bloquear el contenido manipulado. Las redes sociales y en particular Google y Facebook, ya se han comprometido a tomar medidas enérgicas contra las historias falsas que se propagan a través de feeds y grupos, pero hasta ahora han tenido poco impacto. Siendo este el caso, la proyección final seguirá dependiendo de los usuarios. Pero mientras los usuarios no sean educados en señalar noticias falsas, dicho contenido continuará penetrando en línea y será consumido por lectores desprevenidos y sin discernimiento.

- Los actores de amenazas utilizarán tecnologías de aprendizaje automático para expandir sus técnicas de evasión.

El aprendizaje automático puede ser una herramienta poderosa, pero no es infalible. Aunque los investigadores ya están investigando las posibilidades del aprendizaje automático para controlar el tráfico e identificar posibles exploits zero-day no es exagerado pensar que los ciberdelincuentes usarán la misma capacidad para adelantarse a las vulnerabilidades zero-day.

- Muchas compañías tomarán medidas definitivas sobre el Reglamento General de Protección de Datos.

La Unión Europea (UE) finalmente lanzará el GDPR en mayo de 2018, con un gran impacto esperado en el manejo de datos de las empresas que se comprometen con los datos de los ciudadanos de la UE, incluso si dichas empresas están fuera de Europa.

Por lo tanto, las empresas que se despierten con la aplicación de GDPR encontrarán la importancia de contar con un oficial de protección de datos (DPO) dedicado que pueda encabezar el procesamiento y la supervisión de los datos. Las empresas deberán revisar su estrategia de seguridad de datos, incluida la clasificación de la naturaleza y la distinción de los datos de la UE de los datos asociados con el resto del mundo.

- Las aplicaciones y plataformas empresariales estarán en riesgo de manipulación y vulnerabilidades.

Se espera seguir viendo fallos de seguridad en las plataformas de Adobe y Microsoft. Sin embargo, lo que será particularmente interesante es el enfoque renovado en las vulnerabilidades del navegador y del lado del servidor.
Durante años, las vulnerabilidades de los complementos conocidos de los navegadores como Adobe Flash Player, Java Oracle y Microsoft Silverlight han sido atacadas. Sin embargo, en 2018 las debilidades en los motores de JavaScript afectarán a los navegadores modernos. Desde los problemas de bloqueo de V8 de Google Chrome hasta Chakra de Microsoft Edge, las vulnerabilidades del navegador basadas en JavaScript tendrán más apariencias en 2018 dado el amplio uso del script en la web.

También se prevé que los exploits de Samba que entregan ransomware serán mayores en 2018.

4.5 Check Point

- La motivación financiera de los ataques de IoT.

Los ataques masivos a redes IoT crecerán debido a que las capacidades de muchos de los dispositivos serán aprovechadas por los cibercriminales para la creación de marcos de desarrollo, para realizar minado de criptomonedas y para el envío de SPAM masivo distribuido. Además como uno de los nuevos casos de uso, podrán realizar ataques DoS orquestados o bien conseguir acceso a información personal.

- La extorsión a través del cibercrimen.

Aumentará cada vez más la extorsión para recuperar datos encriptados de los equipos que hayan sido comprometidos. Los cibercriminales buscarán atacar grandes servicios o compañías con tal de obtener beneficios mayores, usando para ello ataques dirigidos especialmente para afectar a grandes infraestructuras.

- Ransomware.

El ransomware será parcialmente reemplazado por la minería de criptomonedas. 2017 ha visto un incremento significativo en el valor de las denominadas criptodivisas, creando una gran oportunidad para los cibercriminales. Para minar criptodivisas de forma efectiva y lucrativa es necesaria una gran capacidad de cómputo, que es exactamente lo que una botnet proporcionaría.

- Ataques dirigidos a los sistemas de punto de venta (POS).

Ataques de DDoS y descubrimiento de vulnerabilidades POS serán objetivos durante este 2018, convirtiendo a los servicios de venta en un objetivo lucrativo, utilizando estos puntos de entrada para ataques dirigidos o robo de credenciales, información personal o datos financieros de los clientes que utilicen esos servicios.

4.6 ESET

- La revolución del ransomware.

A medida que el Internet de las cosas (IoT) conectadas aumenta, crecerá la superficie de ataque con dispositivos en red y sensores integrados en elementos y contextos inesperados: desde routers, televisores, hasta juegos y marca-pasos. Aumentarán la cantidad de servicios que pueden verse afectados por el malware.

- Aumentan los ataques a infraestructuras críticas.

Los casos de ciberamenazas que afectan a la infraestructura crítica han sido noticia importante en 2017 y seguirán siéndolo en 2018 a medida que la infraestructura de ataque crece con la incorporación de dispositivos cada vez más interconectados.

- Ataques a la democracia.

Las recientes elecciones y movimientos políticos han planteado numerosas cuestiones de seguridad, siendo la más importante hasta qué punto un ciberataque puede influir en el proceso electoral.

- Condena para el cibercrimen.

La investigación de malware ha demostrado ser útil para la aplicación de la ley en la guerra contra el delito cibernético, se esperan más casos parecidos debido a la violación de las leyes dentro del ámbito telemático y una revisión de las políticas que regulan esto.

- La información personal.

Los datos son la nueva moneda para los consumidores que esperan disfrutar de software a bajo coste o sin coste, lo que lleva a los proveedores a ingresar al negocio de recolección de datos, aumentando los riesgos relacionados con la privacidad de datos recogidos.

5 Conclusiones

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

- El machine learning y la inteligencia artificial tendrán un papel determinante tanto para la detección como la ejecución de ciberataques.
- El ransomware seguirá siendo una pandemia y diversificará sus objetivos, dirigiéndose hacia grandes servicios y organizaciones.
- Los dispositivos IoT serán objetivo de cada vez más ataques debido a su valor una vez hayan sido comprometidos.
- Aumentarán los ataques dirigidos (APT) contra sistemas industriales e infraestructuras críticas.
- Será un año de especial interés para los procesos relacionados con la política en el ámbito de la seguridad informática.

6 Glosario

aplicaciones serverless:	Tipo de arquitectura que habilita la ejecución de una aplicación mediante contenedores efímeros y sin estado que son creados en el momento en el que se produce un evento que dispare dicha aplicación. Contrariamente a lo que sugiere el término, serverless no significa «sin servidor», sino que éstos, se usan como un elemento anónimo más de la infraestructura, apoyándose en las ventajas del cloud computing.
APT:	Siglas de la expresión inglesa Advanced Persistent Threat (Amenaza Persistente Avanzada). Conjunto de procesos informáticos, sigilosos y continuos, dirigidos a penetrar la seguridad de una entidad específica.
BEC:	Siglas de la expresión inglesa Business Email Compromise (Correos Electrónicos Corporativos

	Comprometidos). Correos electrónicos dentro del ámbito empresarial que se han visto comprometidos generalmente por ataques dirigidos.
BIOS:	Acrónimo de la expresión inglesa Basic Input Output System (Sistema Básico de Entrada/Salida). Firmware instalado en un ordenador personal, es el primer programa que se ejecuta cuando se enciende.
bitcoin:	Moneda virtual e intangible. Se asemeja al dinero en efectivo, solo que no se puede tocar en ninguna de sus formas como ocurre con las monedas o billetes.
bot:	Contracción de robot. Tipo de programa informático autónomo que es capaz de llevar a cabo tareas concretas e imitar el comportamiento humano

	diseñados en cualquier lenguaje de programación.
botnet:	Conjunto de máquinas infectadas por malware que son usadas de forma automática y conjunta para la realización de acciones criminales.
CaaS:	Siglas de la expresión inglesa Cryme as a Service (Crimen como Servicio). Modelo de negocio ofrecido por los cibercriminales en el que se profesionaliza la utilización de herramientas informáticas.
CEO:	Acrónimo de la expresión inglesa Chief Executive Officer (Oficial Ejecutivo en Jefe). Persona con la más alta responsabilidad dentro de una corporación anglosajona.
criptodivisa:	Medio digital de intercambio, también denominado criptomoneda, criptodivisa o criptoactivo. La primera

	criptomoneda que empezó a operar fue el bitcoin en 2009 y, desde entonces, han aparecido muchas otras con diferentes características y protocolos como Litecoin, Ethereum, Ripple...
deep web:	Término empleado para referirse a todas las páginas de Internet que no están indexadas por los motores de búsqueda del Internet que conocemos y en el que navegamos todos los días.
DoS:	Acrónimo de la expresión inglesa Denial of Service (Denegación de Servicio). Es un ataque a un sistema de red que provoca que un servicio sea inaccesible. El problema principal, y más importante, es la pérdida de conectividad de la red por el consumo del ancho de banda.
DDoS:	Siglas de la expresión inglesa Distributed Denial of Service. (Denegación de Servicio

	Distribuido). Ataque a un sistema que causa que un servicio o recurso sea inaccesible desde fuentes diferentes, haciendo que este ataque sea complicado de trazar.
DPO:	Siglas de la expresión inglesa Data Protection Officer (Delegado de Protección de Datos). Figura obligatoria que aparece en la regulación europea sobre Protección de Datos (GDPR).
exploit:	Fragmento de software, de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado
feed:	Documentos con formato RSS o Atom (basados en XML). Suelen ser titulares de noticias o notas, generalmente con un resumen del

	contenido y suelen usarse en blogs, sitios de noticias y demás.
GDPR:	Siglas de la expresión inglesa General Data Protection Regulation (Regulación europea sobre Protección de Datos). reglamento europeo mediante el cual pretenden fortalecer y unificar al alza la protección de datos todos los paises de la UE .
hacktivismo:	Acrónimo de hacker y activismo. Se entiende por hacktivista aquella persona que usa herramientas digitales (legales, ilegales o legalmente ambiguas) persiguiendo fines políticos.
hivenet:	Botnets construidas con dispositivos zombies con conjuntos de dispositivos inteligentes comprometidos para crear ataques más efectivos.
IA:	Acrónimo de inteligencia artificial, también llamada inteligencia

	computacional, es la inteligencia utilizada por las máquinas.
IIoT:	Siglas de la expresión inglesa Industrial Internet of Things (Internet de las cosas en el ámbito industrial). Concepto que se refiere a la interconexión digital de objetos industriales con Internet.
infraestructura operacional:	Infraestructuras que prestan los servicios y operaciones y que llevan a cabo la lógica ejecutada.
infraestructura crítica:	Infraestructuras estratégicas para un país, las que prestan servicios esenciales a la sociedad, cuya sustitución o reemplazo no presenta alternativa posible.
IoT:	Siglas de la expresión inglesa Internet of Things (Internet de las cosas). Concepto que se refiere a la interconexión digital de objetos cotidianos con Internet.

keylogger:	Software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado para registrar la información sin que el usuario lo note.
machine learning:	Disciplina científica del ámbito de la Inteligencia Artificial que crea sistemas que aprenden automáticamente, pudiendo identificar tipos de patrones complejos en millones de datos de forma más concreta por ellos mismos.
malware:	Contracción de malicious software (software malicioso). Tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.
malware polimórfico:	Código que se sirve de un motor para mutarse a sí mismo mientras mantiene su algoritmo original

	intacto. Esta técnica es utilizada comúnmente por virus informáticos y gusanos para ocultar su presencia e identificación.
phishing:	Técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.
POS:	Acrónimo de la expresión inglesa Point of Sale (Punto de Venta). Punto de contacto del consumidor con las marcas o productos para su compra.
proxy:	Equipo intermedio que se usa en la comunicación entre otros dos equipos finales.
RaaS:	Siglas de la expresión inglesa Ransomware as a Service

	(Ransomware como Servicio). 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 remover esa restricción.
Samba:	Implementación de código abierto del protocolo Server Message Block (SMB). Permite la interconexión de redes Microsoft Windows, Linux, UNIX otros sistemas operativos juntos, permitiendo el acceso a archivos basados en Windows y compartir impresoras.
SPAM:	Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

swarmbot:	Enjambre de robots que pueden ser programados para seguir unas reglas muy simples, pero que permiten resolver problemas colectivamente que ningún robot podría resolver individualmente.
UEFI:	Acrónimo de la expresión inglesa Unified Extensible Firmware Interface (interfaz de unificada de firmware extensible). Sistema que reemplaza a la BIOS en los sistemas modernos.
waterholing:	Táctica empleada durante la realización de campañas de ataques dirigidos donde la distribución del APT se realiza a través de una web de confianza que suele ser visitada por los empleados de la empresa o entidad objetivo.
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.

7 Documentación de referencia

[1] Personal de FortiNet. <<*2018 FortiGuard Threat Predictions*>>. Hub de Fortinet, noviembre de 2017. Disponible en línea: http://hub.fortinet.com/enterprise-security/2018-fortinet-threat-predictions (Fecha de consulta, 01/03/2018).

[2] Personal de McAfee. <<*2018 Threats Predictions*>>. McAfee Labs Reports, noviembre de 2017. Disponible en línea: https://www.mcafee.com/us/resources/misc/infographic-threats-predictions-2018.pdf (Fecha de consulta, 01/03/2018).

[3] Personal de Kaspersky. <<*Boletín de Seguridad Kaspersky: KASPERSKY LAB PREDICCIONES SOBRE AMENAZAS PARA EL 2018*>>. Kaspersky Secure List, noviembre de 2017. Disponible en línea: https://securelist.lat/files/2017/11/KSB_Predictions_2018_sp.pdf (Fecha de consulta, 01/03/2018).

[4] Personal de TrendMicro. <<*Paradigm Shifts*>>. Web oficial de TrendMicro, diciembre de 2017. Disponible en línea: http://www.trendmicro.es/media/misc/paradigm_shifts.pdf (Fecha de consulta, 01/03/2018).

[5] Equipo de investigación de CheckPoint. <<*What Lies Ahead? Cyber-Security Predictions for 2018*>>. Blog de Check Point, diciembre de 2017. Disponible en línea: https://blog.checkpoint.com/2017/12/13/lies-ahead-cyber-security-predictions-2018/ (Fecha de consulta, 02/03/2018).

[6] Personal de ESET. <<*Tendencias en ciberseguridad en 2018. El costo de nuestro mundo conectado*>>. We live Security, diciembre de 2017. Disponible en línea: https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf (Fecha de consulta, 02/03/2018).