ágoraSIC Centro de Conocimiento en Ciberseguridad


# ¿Cómo van a evolucionar los ciberataques en 2017?

**La revista SIC ha formulado esta pregunta a 107 organizaciones (empresas y centros de servicio públicos y privados), que constituyen el grueso del sector de oferta de Ciberseguridad en España. De sus contestaciones puede deducirse que, además de aumentar las tipologías ya vistas en 2016 y años anteriores, la IoT entra con fuerza como objetivo de los atacantes y con ella sectores hasta ahora no especialmente "trabajados" por la delincuencia.**

* Es posible obtener una versión en pdf de este especial rellenando el formulario disponible en www.revistasic.com

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?

## ACCENTURE

**Álvaro del Hoyo**
Manager, Accenture Security,
Iberia Cyber Defense Offering Lead

"Durante el año 2017 seguiremos viendo cómo el factor humano, sea por errores de diferente tipo o por la cibercandidez frente a la ingeniería social, seguirá siendo el elemento común de la mayoría de los ciberataques relevantes. La principal razón para ello es que las organizaciones siguen sin hacer un adecuado ejercicio de correlación entre sus principios de seguridad y las habilidades y comportamientos hacia los que deben dirigirse los esfuerzos de cambio cultural en materia de ciberseguridad.
Veremos cómo se siguen dando incidentes de espionaje entre Estados, el crecimiento en número y diversidad de los ataques de ransomware, la utilización ilegítima del Internet de las cosas y los ataques lógicos a los cajeros automáticos. Seguirá al alza el compromiso de datos personales y medios de pago en los sitios de comercio electrónico y comenzaremos a ver casos en los que habrá sido determinante la explotación de vulnerabilidades de soluciones de gestión de APIs y entornos con contenedores de aplicaciones y microservicios. Seremos testigos también de ataques en sectores que hasta ahora no habían despertado demasiado el interés de los cibercriminales como puede ser el caso del transporte aéreo y el marítimo".

## A10 NETWORKS

**Juan Muñoz**
Country Manager para España y Portugal

"Veremos que los ataques DDoS batirán nuevos records de volumen, especialmente con la participación de dispositivos IoT infectados por *malware* como ocurrió con la botnet Mirai. También serán más devastadores al atacar a la capa de infraestructura, incluyendo por ejemplo los proveedores de servicio DNS, como en el caso de Dyn en 2016. Los elementos de control industrial, como presas, plantas potabilizadoras, nuevos automóviles autónomos, etc, serán nuevos objetivos de ataques dirigidos. Por último, las amenazas de "ransomware" serán más frecuentes y serias que el pasado año, donde se constató un notable crecimiento. Estas utilizarán cada vez más el cifrado SSL para evitar las barreras de seguridad corporativas, usando entre otros medios las redes sociales para propagarse".

## AIUKEN GLOBAL SOLUTIONS

**Juan Miguel Velasco López-Urda**
CEO

"El crecimiento de migración a la Cloud de las empresas grandes y medianas traerá un aumento de los ataques hacia los datos y servicios Cloud,muchas empresas migran sin tener en cuenta la seguridad (CASB, IRM, etc), los ataques serán principalmente robo de datos y ataques a infraestructuras, lo que sumado al aumento del IoT potenciará la multiplicación de botnets, al servicio de ataques de DDoS contra protocolos y servicios no habituales como DNS, NTP, etc. Además veremos el renacimiento de viejos ataques con vulnerabilidades ya conocidas pero que serán explotadas en los nuevos sistemas IoT domésticos, de transporte y SCADA que implementan sistemas con viejas vulnerabilidades listas para ser explotadas. El Security by design sigue siendo un desconocido para los IoTs..."

## AJOOMAL

**Jorge Puerta**
Director Comercial

"Los ataques de *ramsomware* seguirán estando en el día a día de los clientes, con una difusión exponencial por la dificultad de su detección y de remediación de sus efectos. También seguirán en plena expansión los ataques de DNS, corazón de la red; actualmente en muy pocos sitios están preparados para este tipo de ataques, los cuales son demoledores. Por último, la fuga de información sigue siendo un ataque contra la propiedad de los datos de las empresas y organismos, y se está invirtiendo mucho para la remediación por parte de fabricantes de soluciones de DLP y de monitorización y supervisión del comportamiento de los usuarios internos".

## ALL4SEC

**Alfonso Franco**
CEO & Managing Director

"La extorsión en línea y los ataques de seguridad dirigidos al entorno político han copado los medios de comunicación durante 2016. Algunos términos como ransomware o hacktivismo se han hecho desgraciadamente habituales. La progresiva incorporación de dispositivos IoT, la utilización de terminales móviles para llevar a cabo operaciones de negocio (como por ejemplo están impulsando las nuevas tendencias de Fintech) nos están llevando a un nuevo escenario de la seguridad en el que el comportamiento de las personas y la protección de los *endpoint* juegan un papel fundamental. En 2017 debemos esperar que estas técnicas de malware continúen extendiéndose, con ataques cada vez más sofisticados, centrados en el empleado y en sus dispositivos como vector de entrada a las organizaciones".

## ALLOT

**Rafael García de la Rasilla**
Directo de Canal y de Cuentas Proveedores de Servicios

"La tendencia exponencial del Ransonware va a ser sin duda uno de los retos en este año; de hecho prevemos una evo-

lución hacia los dispositivos móviles y por ello los operadores están ampliando su oferta de servicios a otorgar seguridad desde la red. Seguiremos con un constante crecimiento de ataques phishing y tipo botnet aprovechando las brechas del ecosistema IoT".

## AndalucíaCERT

**Eloy R. Sanz Tapia**
Gabinete de Seguridad y Calidad.
Servicio de Planificación Tecnológica.
Dirección General de Telecomunicaciones y Sociedad de la Información.
Consejería de Empleo, Empresa y Comercio.
JUNTA DE ANDALUCÍA

"Aparte de la continuación de las amenazas actuales, que tan buen resultado están dando, como el ransomware o los ataques de alquiler, probablemente veamos un crecimiento en el secuestro de servicios en la nube (como el reciente caso de las bases de datos MongoDB) y en los ataques a las "infraestructuras críticas de la red", como el sistema DNS o los puntos neutros de intercambio de tráfico (quizá veamos este año un país fuera de Internet por un ataque, y no por decisión propia). Los usuarios seguirán siendo el foco de atención para los ataques, junto con los dispositivos básicos (los habitantes de la Internet de las cosas) y ambos serán usados como canales y amplificadores para ataques a otros objetivos. Por parte de AndalucíaCERT, formación, organización y colaboración son nuestros antídotos de cabecera".

## ASTREA LA INFOPISTA JURÍDICA

**Nacho Alamillo Domingo**
Director

"El año se presenta absolutamente interesante en términos de los denominados servicios de confianza, elementos fundamentales para el aseguramiento de los procesos de negocio. Quizá el más atractivo, y esperado, servicio de confianza sea la creación remota de la firma electrónica cualificada con claves centralizadas, que sin ninguna duda se pondrá en funcionamiento este 2017 en España, permitiendo a millones de personas actuar en el tráfico jurídico - por ejemplo, en las relaciones con las Administraciones Públicas, gracias a Cl@ve Firma, de forma más eficiente. Es indudable que semejante tipo de servicio será objeto de ciberataques, y que, en caso de éxito en el robo de las claves, el impacto sería desastroso, por lo que resultará imperativo emplear tecnologías verdaderamente seguras, algo que no en todos los casos está sucediendo. Más preocupantes, sin embargo, serán ataques dirigidos al engaño del usuario, con el objeto de que el mismo cree una firma electrónica cualificada respecto a un contenido malicioso; algo que –leyendo los estándares aplicables– puede que esté al alcance de todo el mundo".

## ARBOR NETWORKS

**Gonzalo Oltra**
Director de Ventas para Iberia

"Los ataques masivos alimentados por miles de millones de dispositivos conectados seguirán evolucionando durante 2017.
Cada vez veremos más ataques y muy diferentes a lo que hemos estado sufriendo, serán cada vez de más capacidad, más complejos y de mucha más intensidad tanto en tamaño como en número. Tanto los ciberataques dirigidos al robo de datos y documentación, como los de denegación de servicio o los ataques selectivos de propiedad intelectual seguirán existiendo y avanzando, pero se deben 'securizar' al máximo las redes y las inversiones contra tales amenazas serán un recurso importante con un retorno de inversión claro que proporcionará una buena salud a nuestra red".

## ARROW ECS

**Gorka Sainz Rodríguez**
Security Presales Manager

"El *ransomware* continuará siendo un negocio lucrativo para los *hackers*, pero es en el IoT donde tienen un verdadero filón.
El reciente ataque a Dyn dejó patente que no se pone el suficiente foco en la protección de estos nuevos dispositivos conectados a internet.La ingeniería social vuelve a estar de moda, recordando la importancia de proteger no sólo la infraestructura TI, sino también el acceso físico y, sobre todo, la necesidad de invertir en la educación de los usuarios".

## ATOS

**Arancha Jiménez**
Responsable del Área de GRC y Ciberseguridad

"Los ciberataques en 2017 incrementarán considerablemente respecto a años anteriores siendo más complejos y avanzados.
Teniendo en cuenta que los ataques dirigidos ocuparán el top del *ranking*, seguidos de los ciberataques orientados a aquellos entornos con un alto grado de exposición y donde todavía no se han implementado los controles de seguridad apropiados (por ejemplo, IoT, ICS…). No debemos olvidar la necesidad de implementar medidas de seguridad en aquellos proveedores que dan servicios cloud, puesto que otro de los objetivos de los ciberataques para el próximo año serán estos proveedores de servicios".

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?

## BARRACUDA NETWORKS

**Miguel López**
Country Manager Iberia

"En 2017 tres importantes ciberamenazas cobrarán, lamentablemente, mucho mayor protagonismo del que han tenido hasta la fecha: 1) Internet de las cosas: el crecimiento exponencial de dispositivos conectados y con una muy escasa seguridad por defecto es el caldo de cultivo perfecto para ataques cada vez más frecuentes y extensivos. Esperemos que en este año no veamos el gran apagón de internet debido a esto; 2) Cloud: a medida que la adopción de la misma se incrementa crece también su interés para la industria del malware. En 2017 veremos cómo muchas de las grandes brechas de seguridad suceden en nubes privadas o públicas no suficientemente protegidas; y 3) Ciberterrorismo y ciberguerra: Internet abre un nuevo campo de batalla (nunca mejor dicho) que no por ser digital ha de ser menos dañino en vidas y recursos. Protegernos frente a un 11M electrónico es responsabilidad tanto de las AAPP como del sector privado".

## BITDEFENDER

**Horatiu Claudiu Bandoiu**
Channel Marketing Manager SE y LATAM

"2017 será un año muy animado porque ya asistimos a un estado de madurez de los actores/atacadores. Según nuestras expectativas, cabe destacar un incremento en el número y sofisticación de los ataques de los estados, usando APTs. Los principales poderes mundiales también van a mostrar su fortaleza en el ciberespacio (ya empezó la pugna entre Rusia y EEUU…); aparecerán nuevos *exploit kits* que proporcionarán nuevos vectores de ataque para el ransomware. Se verán ataques *ransomware multichannel* (multi-vector) dirigidos a las empresas, pero los usuarios domésticos van a sufrir igualmente en 2017; en el mismo ámbito de la cibercriminalidad, anticipamos crecimiento en los robos de identidad y del fraude usando tarjetas y nuevos métodos de pago; respecto a la explosión de los dispositivos IoT –de los que ya hemos visto ataques impresionantes usando este vector- en 2017 esperamos muchas "exploraciones" en este ámbito porque los fabricantes de estos dispositivos y los usuarios prácticamente ignoran la componente de seguridad".

## BT SECURITY IBERIA

**David Fernández Granado**
Director Comercial

"2017 será un año puente entre la vieja forma de hacer las cosas en materia de ciberataques y el "Armagedón cibernético" de 2018 por la entrada de regulaciones importantes que si bien tienden a crear un mercado digital más justo dando relevancia a la ciberseguridad, también incentiva de alguna manera al *ecrime* para incrementar su ámbito de actuación, tanto en cantidad como en calidad, buscando maximizar su beneficio "comercial". Estos se apoyarán en los nuevos medios que tienen a su alcance (IoT, redes sociales, nube) para la obtención de información sensible que luego pueda ser comercializada mediante chantajes a empresas frente a las agencias de protección de datos o simplemente generando indisponibilidades de servicios esenciales para la sociedad digital. Emergerá el "planting" como actividad de soborno a personal interno con mucha fuerza como elemento 'troyanizador' físico que permita el éxito de los ciberataques adicionalmente a las tácticas y técnicas que hemos estado viendo durante el 2016".

## BLUELIV

**Daniel Solís**
CEO y Fundador

"En 2017 las ciberamenazas ocurrirán con más frecuencia y serán mucho más agresivas. Seguiremos con infecciones y propagación del malware, teniendo un gran foco en la cibersextorsión, pudiendo afectar a todo tipo de plataformas y verticales: Smart cities, IoT, infraestrcuturas críticas, móviles, drones, etc. Esto se verá dinamizado por la facilidad de cobro y movimiento de divisas a través de criptomonedas como bitcoin. Además, el anonimato mediante redes tipo tor continuará contribuyendo a la ocultación de los orígenes de los ataques y dificultando la trazabilidad.
Por otro lado, el malware será especialmente dañino contra entidades financieras, creando nuevos caballos de Troya bancarios más evolucionados y de difícil detección temprana. En cuanto al "crime-as-a –service" en sus diferentes facetas será una industria cada vez más creciente. Hasta el punto de tener más oferta y especialización según tipo de delitos a contratar. Esto se verá agravado por la colaboración entre bandas criminales, en modelos en los cuales se compartan beneficios, tal y como ya ocurriera con Vawtrak y Moskalvzapoe".

## CA TECHNOLOGIES

**Jacinto Grijalba**
Estratega de Soluciones de Seguridad

"Los cambios derivados de la transformación digital, la adopción creciente de tecnologías híbridas y la llegada de nuevos marcos regulatorios como GDPR, demandan un modelo de trabajo basado en **DevSecOps**, donde el desarrollo y la operación de nuevos servicios no sólo se base en metodologías ágiles, sino que añada una capa de seguridad que mejore la experiencia y confianza de los consumidores. Asimismo, el robo de identidades privilegiadas no controladas ha destacado como denominador común en los últimos ciberataques, convirtiéndose en una de las principales brechas de seguridad de las organizaciones que requerirá medidas específicas de protección".

## CAPGEMINI ESPAÑA

**Jorge Hurtado**
Director de Servicios de Ciberseguridad

"Durante 2017, veremos un incremento de los ataques sobre y desde dispositivos IoT, donde algunos fabricantes seguirán practicando la "Ciber-inseguridad por diseño". Por otro lado, el endurecimiento de las sanciones por incumplimiento en la nueva Regulación de Protección de Datos Europea, hace pensar que próximamente nacerá el "RamsomGDPRware" dirigido a grandes instituciones a las que se extorsionará ante la amenaza de la sanción y/o notificación".

## CCN

**Javier Candau**
Jefe del Departamento de Ciberseguridad

**1.** "Los asociados al **ciberespionaje** (tras las elecciones en EE.UU. algunos de estos ataques han tenido mucho eco mediático aunque los mismos se vienen sufriendo durante años en las AAPP y empresas estratégicas) con actores esponsorizados por estados; los orígenes y la complejidad de los mismos es muy diversa y lamentablemente nuestras organizaciones no están preparadas para responder a los mismos. Además, se espera mayor variedad de ataques sobre plataformas móviles de personas clave en las organizaciones antes mencionadas.
**2.** Los relacionados con el **cibercrimen**; se espera que incremente su actividad y selectividad hacia objetivos más rentables en la infección mediante variantes de ransomware, variantes de código dañino para medios de pago, la "estafa del CEO" (CEO Fraud) y ataques complejos al sector financiero, denegaciones de servicio distribuidas usando internet de las cosas y venta de servicios a terceros (redes de botnets, herramientas de ataque,…)
**3.** Los relacionados con **grupos hacktivistas**, tanto de origen nacional como internacional; continuarán los ataques por denegación de servicio y las desfiguraciones. Además, hay que tener en cuenta la permanencia/aparición de identidades con elevadas capacidades técnicas para ejecutar acciones de alto impacto por razones ideológicas y el uso de código dañino para extorsión.
**4.** Con relación al **ciberyihadismo**, se mantendrá limitado a la propaganda y a la presencia de identidades en redes sociales, así como la realización de ataques no complejos contra objetivos de bajo perfil. Eventualmente se podrían aprovechar errores de la parte defensiva y la asociación o contratación de capacidades relacionadas con el cibercrimen.
Desde el punto de vista defensivo se debe mejorar en la capacidad de vigilancia de las redes ante ataques complejos, en la configuración segura de los dispositivos móviles y su monitorización, en la configuración segura de los dispositivos Internet de las cosas (IOT) y en la vigilancia de los sistemas de control en general (plantas industriales, sistemas de distribución, sistemas de salud, edificios…) pues la seguridad no se ha considerado ni en su diseño ni en su implementación. Es además necesaria incrementar la concienciación de los usuarios en el uso de los dispositivos y los elementos conectados a Internet".

## CENTRO DE CIBERSEGURIDAD INDUSTRIAL-CCI

**José Valiente**
Director

"Los ciberataques durante el 2017 darán un salto cuántico en cuanto a sus capacidades, no se necesitarán nuevos mecanismos sofisticados, solamente controlar las recientes, potentes y vulnerables plataformas de Smart OT (Tecnologías de Operación Inteligentes) que permitirán desarrollar ataques dirigidos y personalizados. En el 2016 se recibió, a través del *malware* Mirai, el primer aviso del tsunami que llegará en 2017, y arrasará multitud de infraestructuras críticas públicas y privadas que no tengan capacidades de resiliencia para resistir y recuperarse".

## CESICAT

**Xavier Gatius Garriga**
Director General del Centro de Seguridad de la Información de Cataluña

"El despliegue cada vez mayor de redes de dispositivos IoT podría propiciar en este 2017 una mutación de los canales habituales por medio de los cuáles se materializan determinados ciberataques. El *malware* y los ataques DDoS podrían ser candidatos a este cambio de escena, en especial aquellos de gran intensidad en el caso de los DDoS. Infraestructuras críticas, salud y energía probablemente sean los entornos con mayor beligerancia y la industria del entretenimiento y los videojuegos los candidatos más recurrentes para determinadas tipologías de ataques".

## CHECK POINT

**Mario García**
Director General para España y Portugal

"Durante el año 2017, habrá un aumento importante de ciberamenazas que no atacarán a las empresas, sino a los individuos que trabajan para ellas. De hecho, según nuestras predicciones uno de cada cinco empleados descargará *malware* en las redes corporativas durante este año. Serán ataques sofisticados que se propagarán cada vez más a través de las redes sociales, por lo que las compañías deben educar y concienciar a su personal en materia de ciberseguridad. Las amenazas más comunes a las que se enfrentarán las compañías serán el *ransomware*, el *phishing* y el *malware* móvil".

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?

## CISCO

**Eutimio Fernández**
CyberSecurity Leader Spain & Portugal

"La desaparición de los grandes exploit kits (Angler, Nuclear, Neutrino) creará nuevos grupos de ciber-delincuentes más pequeños, numerosos y focalizados, que harán necesario el uso de más inteligencia para una defensa proactiva. Las técnicas como el *malvertising* seguirán siendo habituales para la infección con malware, así como el uso de los dispositivos IoT para ejecutar ataques, ya que todavía queda mucho por hacer respecto a la seguridad IoT. Asimismo, las conexiones Open Authentication con el Cloud suponen un nuevo riesgo, mientras que el spam volverá a niveles récord como los de hace 10 años mediante botnets como Necurs. Por último, el ransomware, muy de moda durante 2016, seguirá evolucionando con la intención de ser más lucrativo y veremos casos de secuestro de redes enteras con nuevas variantes".

## CITRIX SYSTEMS IBERIA

**Santiago Campuzano**
Country Manager

"Los ciberataques estarán más que nunca orientados a afectar a la transformación digital de las organizaciones, centrándose en Cloud, Mobility, Big Data o IoT. Ya sea mediante el bloqueo de entornos de nube con ataques de DDoS, robos o adulteraciones de la información de las organizaciones modificando sus capacidades de decisión y el uso de esa "autopista insegura" que es IoT y, por extensión, las plataformas de movilidad inseguras. Por ello, garantizar la disponibilidad de las plataformas y su 'securización' evitando los citados ataques DDoS, limitar las lagunas de seguridad en dispositivos no gestionados o no virtualizados, y tener plataformas de gestión del dato que faciliten la gestión y la 'securización' de los datos de los usuarios con plataformas de File Sharing va a resultar fundamental. Las actividades para suplantar a los usuarios y extraer información también serán otro de los aspectos a cuidar en 2017".

## CSIRT-CV

**Lourdes Herrero**
Directora

"Las amenazas se trasladarán, una vez más, hacia las mismas tecnologías y plataformas que las preferencias de los usuarios. En este sentido, el problema del *malware* para dispositivos móviles, –mayor en Android, al tener mayor parque–, crecerá y se verá agudizado por el empleo de técnicas como la colusión de APPs maliciosas, que conseguirán reducir la efectividad del aislamiento entre ellas. También veremos aumentar los ataques ligados a dispositivos IoT, al pago por móvil y a los sistemas de control industrial presentes en las infraestructuras críticas. Podemos esperar nuevas variantes *ransom*, ante las que las reglas de protección se mostrarán ineficaces, si se ejecutan explotando una vulnerabilidad del lado del cliente, o entran en éstos a través de *botnets*, que ya estuvieran presentes previamente. Las campañas de APT´s seguirán evolucionando tanto en complejidad como en alcance".

## CONSIST INTERNATIONAL

**Paloma García Piserra**
Gerente

"Según mi punto de vista, los ciberataques continuarán la línea trazada en 2016 mediante el uso de "internet de las cosas". Cualquier elemento (teléfono, coche, electrodoméstico, etc.) conectado a internet se puede convertir en un soldado perteneciente a un ejército de robots, los cuales posiblemente puedan ser utilizados para lanzar ataques colectivos con el fin de provocar una "denegación de servicio". Este ataque puede provocar un caos en las comunicaciones colapsando la red de cualquier organismo, aislándolo del resto del mundo. No hay que olvidar que el crecimiento y la complejidad de los ataques internos dentro de las compañías continuarán incrementándose en 2017".

## COUNTERCRAFT

**David Barroso**
Socio

"El año 2016 supuso un importante cambio de tendencia en la mayoría de ataques con objetivos económicos: en 2017 apenas veremos caballos de Troya bancarios o *phishing*; es mucho más lucrativo y sencillo utilizar el *ransomware* y concentrar todos los esfuerzos en pocos ataques dirigidos que conlleven el robo de millones de euros (p.ej.: Carbanak, incidencias en SWIFT…). Los administradores de red y de sistemas serán objetivos directos de los ataques (puesto que ellos tienen las llaves de acceso), y algunos de los incidentes serán resultado de extorsiones a los propios trabajadores –los fans de la serie 'Black Mirror' se sentirán identificados– donde las extorsiones por grabaciones sexuales no sólo buscarán dinero rápido".

## CYBERARK

**Albert Barnwell**
Account Manager para España y Portugal

"Creemos que los beneficios de la transformación digital de servicios hacia el cloud no ha pasado desapercibida por los hackers. De la misma manera que se aprovecharán de la inseguridad de los dispositivos IoT para lanzar ataques de gran escala, también utilizarán el Cloud para acelerar la producción de herra-

mientas de ataque. Gracias al nuevo potencial de computación del Cloud y ágil desarrollo, estas herramientas serán cada vez más robustas y difíciles de combatir."

## DAVINCI TI
**Javier Sierra**
Director del área de Seguridad

"Las aplicaciones están dirigiendo la innovación y el crecimiento masivo de datos, resultando en un incremento sin precedentes en el volumen de ataques. La mayor parte de los ciberataques se orientarán a la capa de aplicaciones y a la identidad, con objeto de conseguir acceder de forma fraudulenta a los datos más valiosos de las organizaciones (casi un 75% de las brechas de datos están relacionadas con aplicaciones vulnerables e identidades comprometidas)".

## DELOITTE
**Rubén Frieiro Barros**
Socio Risk

"Como firma especializada en la prestación de servicios de ciberseguridad, creemos que durante 2017 asistiremos a un incremento de los ciberataques, continuando la tendencia alcista vivida durante los dos últimos años. Una mayor adopción de tecnológicas como IoT, machine learning o la evolución de canales de negocio digitales habilitarán nuevos vectores de ataque, cada vez más sofisticados y más dirigidos. También percibimos una mayor preocupación de la alta dirección de las compañías por el impacto (más allá de lo económico) y la resonancia que estos incidentes están teniendo en los mercados y en la sociedad en general. Esto está provocando que las autoridades públicas muestren un mayor interés mediante un incremento de la regulación, la compartición de la información y una búsqueda de la colaboración público-privada en la respuesta".

## DINOSEC
**Raúl Siles**
Fundador y Analista Senior de Seguridad

"¿Y si nos planteásemos que los ataques no tienen que evolucionar significativamente en 2017, porque realmente no se lo estamos poniendo más difícil a los atacantes? Sin embargo, creo que el año 2017 es una muy buena oportunidad para la industria de seguridad informática y nuevas tecnologías para finalmente forzar a todo el planeta a migrar a HTTPS, hacer un uso extensivo y (casi) universal de TLS (especialmente con la versión 1.3), y aprovechar al máximo sus capacidades de autentificación y cifrado, asumiendo que es implementado correctamente."

## EFFICIENT IP
**Yannick Bodin**
Director de Preventa para Iberia y Latinoamérica

"Desde EfficientiP vemos a la seguridad de los DNS como el primer objetivo de los *hackers* para este 2017.Como se ha visto recientemente, la posibilidad de "pegada" es mucho mayor (debido a la estructura de árbol de DNS), con el mismo esfuerzo (p.ej. Yahoo). En esta dinámica los dividiríamos en 3 tipos: 1) Ataques Volumétricos (DoS DNS Directos; Amplificación DNS (DDoS), Reflejo DNS, NXDOMAIN (dominio inexistente); 2) Ataques de goteo (ataques de dominio perezoso, fantasma, y de subdominio aleatorio (RQName); y 3) Aprovechamiento (vulnerabilidad 'día cero'), aprovechamientos basados en DNS, ataque de envenenamiento de la caché DNS".

## ELEVEN PAHTS
## (Telefónica Cybersecurity Unit)
**Pedro Pablo Pérez**
CEO

"Sin duda alguna en 2017 continuarán las campañas de ransomware, ataques distribuidos de denegación de servicio, fugas de información y ataques dirigidos, dado que es la tendencia creciente desde hace 3 años. Por otro lado, estimamos que habrá un mayor volumen de ataques a compañías españolas así como infraestructuras críticas, sin embargo cada vez es más patente que nadie está a salvo en los ciberataques, dado que hay ratios de infección en particulares que superan ya el 2% de terminales y un creciente número de incidentes en PYMES, que sin duda son los eslabones más débiles de la cadena".

## ENCIFRA
**Valle Fernández**
Dirección. EnCifra y SMiDCloud

"En 2017 seguirán siendo vulnerables a los ciberataques los negocios y empresas de todos los tamaños. Dado que el negocio del ransomware es la forma más sencilla y eficaz de generar beneficios, veremos en 2017 no sólo un aumento en el número de ataques sino también en la sofisticación del malware implicado, probablemente con el objetivo de conseguir ataques dirigidos a víctimas más "rentables". A medida que se consoliden las Fintech, aumentará el interés de algunos en atacar a los nuevos servicios financieros para beneficio económico propio. Seguirá habiendo ataques desde Internet contra los sistemas de información de grandes compañías e instituciones, en el primer caso para conseguir materiales vendibles en el mercado negro, y en el segundo caso para desprestigiar a las víctimas por su presunta incapacidad de haberlo sabido evitar. Como en años anteriores, los incidentes causados por "insiders" seguirán sin ser públicos, y habrá que esperar al pleno funcionamiento de la directiva NIS Europea para conocerlos".

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?

## EPOCHE & ESPRI
**Miguel Bañón**
Director

"Nos llama la atención la 'commoditization' o mercantilización de las APT, que pasan de ser rara-avis a meta-APTs, generalizados, automatizados, y con niveles de abstracción y diseño cada vez más complejos, eso sí, sobre productos no evaluados ni certificados".

## ESET ESPAÑA
**Josep Albors**
Director de Comunicación y Laboratorio

"A lo largo de 2017 veremos que los ciberdelincuentes intentar sacar mayor rédito a sus creaciones, intentando interconectar amenazas. El *ransomware* continuará haciendo estragos, también a través de nuestros *smartphones*. Seguirán sacando beneficio de nuestros datos privados y no resultará extraño que los dispositivos IoT se conviertan en protagonistas tanto para realizar ataques de denegación de servicio, como sistemas de almacenamiento y propagación de *malware* o siendo víctima de ataques diseñados. Por último, podremos ver disrupciones importantes en el correcto funcionamiento de Internet. Aprovechando vulnerabilidades presentes en millones de dispositivos se podría impedir a millones de usuarios utilizar servicios *online* comunes como el correo-e o redes sociales, no solo durante unas horas y en una zona limitada sino a escala global y durante un periodo más prolongado. Esto podría causar graves problemas si, además, deja fuera de juego temporalmente servicios críticos de telecomunicaciones u operaciones financieras, algo que en teoría es dificil pero no imposible".

## EVERIS
**Miguel Ángel Thomas**
Director Ejecutivo de Ciberseguridad

"En 2017 se mantendrá como principal amenaza el *ransomware*, se prevé que cada vez exista más sofisticación y que su nivel de mutaciones sean diarios. Asimismo las amenazas provenientes sobre software y protocolos habituales a través del descubrimiento de nuevas vulnerabilidades serán el vector de ataque más habitual, teniendo muy en cuenta cómo pueden impactar no solamente en los Sistemas de Información tradicionales sino también en las Infraestructuras Críticas (que utilizan a bajo nivel muchos de este software base). Las ICe IoT serán objetivos claros de ataque durante este 2017. Por último, la ingeniería social, principalmente para comprometer *insiders*, junto con técnicas de explotación de vulnerabilidades, será el medio principal para realizar ataques dirigidos".

## EXCLUSIVE NETWORKS
**Manuel Cubero**
System Engineer Manager

"Como cada año los ataques incrementan tanto por su número como por su sofisticación. Ataques de moda actuales como los DDoS o ransomware continuarán haciendo estragos y evolucionando, sobre todo estos últimos, que amplían su espectro de actuación a dispositivos móviles y aparecen versiones nuevas que no necesitan descargar fichero para cifrar el equipo. De igual forma y vinculados al incremento de la aceptación y uso de las plataformas *cloud* los nuevos *exploits* tienen un claro enfoque contra los sistemas virtualizados y plataformas *cloud*. Sin duda, lo que empieza a marcar una clara tendencia como objetivo, son los llamados IoT tanto industriales como personales y el uso cada vez de más técnicas sociales en el momento de la distribución e infección. La combinación del *ransomware*, uso de nuevas técnicas sociales y dispositivos IoT personales, dejan ver una clara tendencia de ataques orientados al eslabón más débil de la cadena, los usuarios. Para que una vez conseguido, centrase en el secuestro virtual de equipos y datos ya sean del mismo usuario o escalando en las organizaciones a las BBDD y servidores".

## EY
**Miguel Rego Fernández**
Cybersecurity Leader

"Los cibercriminales van a seguir actuando de una forma no siempre fácil de comprender y de prever. Además de las acciones más frecuentes, como el fraude on-line, el robo económico o de información, se incrementará la probabilidad de ciberataques contra las infraestructuras críticas y contra dispositivos y artefactos, como los coches inteligentes y los sistemas médicos avanzados, que han ido incorporando sensores y conectividad. Sin una ciberseguridad, eficaz y adaptativa, que sea capaz de identificar las nuevas formas en que se desarrollan los ciberataques y evolucionar proporcionando un entorno de control adecuado, no sólo se estará poniendo en riesgo la información y los sistemas sino la propia seguridad de las personas".

## FIBERNET
**Esther Gómez Vidal**
Directora General

"Al mismo ritmo que aparecen novedades tecnológicas que nos permiten facilitar los procesos de negocio también los *hackers* disponen de más mecanismos para llevar a cabo los diferentes tipos de ciberataques. El Instituto Nacional de Ciberseguridad publicaba el año pasado el dato de unos 35.000 incidentes en España, algunos de ellos afectando a infraestructuras críticas para

el Estado. Uno de los objetivos para luchar contra estos ataques es adelantarse a los mismos tratando de analizar el mayor número de vulnerabilidades a las que estamos expuestos, adoptar medidas que robustezcan nuestros sistemas y con mecanismos de detección de esas amenazas para reducir el tiempo de actuación de los *hackers*.

En este sentido estamos trabajando en Fibernet en el lanzamiento de una nueva línea de productos orientada a detecciones tempranas de intrusiones, tanto a nivel físico de acceso a ciertas ubicaciones con restricciones de acceso, detección de manipulaciones en elementos críticos, etc. Todo ello utilizando la fibra óptica como sensor además de como medio seguro de transporte de datos...".

## FIREEYE

**Vesku Turtia**

Regional Sales Manager, Iberia

"Al *ransomware*, la escasez de talento y las amenazas del estado nacional se siguen viendo como problemas a esperar cuando se mira hacia adelante. Veremos un aumento continuo de ataques contra regiones maduras menos seguras, y EMEA es una de ellas. Aumentarán las operaciones cibernéticas motivadas políticamente, que normalmente rodean los conflictos globales o regionales (China, Rusia, ataques de los estados nacionales) y desarrollos agresivos y altamente dinámicos de los ciberdelincuentes que buscan alcanzar metas financieras. Esto significa que el *ransomware*, la adopción rápida de las vulnerabilidades conocidas y el uso de la información robando *malware* continuarán siendo un desafío para la mayoría de las empresas en EMEA en 2017. Igualmente seguiremos viendo actores de amenazas sofisticados financieramente enfocados en estos y otros sistemas críticos y, finalmente, los ataques de interrupción como se ven con Shamoon 2.0 seguirán aumentando".

## FORCEPOINT

**Fabiano Finamore**

Country Manager para Iberia

"El uso masivo de la Inteligencia Artificial activada por la voz humana para tener acceso a la web, a los datos y a las aplicaciones, generará nuevos vectores de ataque y un gran impacto en la privacidad de los datos. Igualmente, la nube se erigirá también en un emergente vector de ataque, evidenciándose el desafío de asegurar las infraestructuras cloud. Respecto al incremento de las amenazas internas, una nueva amenaza interna –incentivada por las corporaciones– podría colisionar con los datos de los clientes, las ganancias corporativas y otros objetivos de desempeño. Finalmente, la convergencia del cumplimiento y la protección de datos y las demandas de GDPR podrían elevar más los costos empresariales a medida que se implantan los nuevos controles de protección de datos y los entes concernidos tratan de resolver el quién, cuándo y cómo de los requisitos para tener acceso a los datos".

## FORTINET

**Acacio Martín**

Director Regional para España y Portugal

"Prevemos una mayor sofisticación en los ataques automatizados, emulando mucho mejor el comportamiento humano, así como un incremento en los ataques diseñados para explotar vulnerabilidades de los millones de dispositivos inseguros IoT, que serán la vía de entrada para atacar, entre otros, a los proveedores Cloud que concentran una muy alta actividad. Por otro lado, la SmartCity estará en el punto de mira de los *hackers*, debido al incremento de sistemas de automatización y gestión".

## F5 NETWORKS

**Álex López de Atxer**

Country manager

"Nuestro SOC de Varsovia detectó un incremento del 100% en los ataques tipo DDoS durante 2016, y creemos que esta tendencia, empujada por la proliferación de dispositivos IoT, continuará este año. Ante la creciente variedad de ataques tipo DDoS (fragmentación UDP, DNS y NTP Reflections o inundaciones UDP y Syn), la solución pasa por detectar las irregularidades que se producen en el tráfico, con el objetivo de ser capaces de identificar si se está sufriendo un ataque y poder reaccionar con la mayor rapidez".

## GEMALTO

**Alfonso Martínez Díaz**

Director Regional de Ventas España y Portugal

"En 2017, se extenderá un tipo de ataques más intrincados, complejos y no detectados: los ataques a la integridad de los datos. Tendrán dos motivos principales: ganancia financiera y/o manipulación política. La integridad de los datos es una promesa o garantía de que solo los usuarios autorizados pueden modificar o acceder a la información. Los ataques a la integridad de los datos comprometen la promesa de que sólo los usuarios autorizados pueden modificar o acceder a la información, con el objetivo de obtener acceso no autorizado para modificar los datos por una serie de motivos ocultos. Es la máxima forma de transformar los datos en armas. Estamos empezando a ver pruebas de que los datos robados se alteran antes de su transición de una máquina a otra, afectando todos los elementos de las operaciones. Los ataques a la integridad de los datos tienen el poder de derribar una empresa entera. Lo que está en juego es la confianza. La toma de decisiones por altos funcionarios del gobierno, ejecutivos corporativos, inversores y consumidores promedio se verá afectada si no pueden confiar en la información que reciben".

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?

## GMV Secure e-Solutions

**Mariano J. Benito**

CISO

"Ha habido y habrá evolución en la tipología de ciberincidentes que se experimentarán en 2017. Este punto ha sido, es y será la única constante que podemos afirmar con absoluta seguridad. Por ello y en todos los casos, las organizaciones deben dotarse urgentemente de equipos especializados con capacidad de detección de incidentes (nuevos y ya conocidos) y de respuesta a incidentes, ya sea mediante colaboradores especializados, ya sea dotándose de medios propios, si es que están disponibles en el mercado.

2017 traerá un aumento de los incidentes derivados de vulnerabilidades y errores de seguridad existentes en los servicios y elementos software que no fueron (peor aún, sean) desarrollados con consideraciones de seguridad embebidas desde su diseño. Ya en 2015 vimos una primera de 0-days en elementos core de nuestros sistemas TI (poodle, heartbleed, drown), y ahora veremos más ataques dirigidos a aplicaciones desarrolladas ad-hoc para las organizaciones, sobre todo para aplicaciones legacy.

Dicho esto, 2017 mantendrá también constante el origen de muchos de los incidentes: el beneficio económico directo para el atacante. En particular, aumentarán los intentos de fraude a corporaciones. Además de nuevos modelos que puedan aparecer, se seguirán explotando los modelos de fraude que ya tienen en uso y que son específicos de cada sector. Las organizaciones que ya han trabajado en detectar, corregir y prevenir el fraude en sus modelos de negocio tendrán en este punto un año menos ajetreados. Las demás tendrán que trabajar en conceptos ya conocidos: vigilancia digital, gestión de vulnerabilidades, inteligencia,…

La evolución de los incidentes no será igual en todos los sectores. Veremos más incidentes en el sector sanitario, de alta sensibilidad para el ciudadano y que hasta el momento no ha sido "suficientemente atendido" por parte de los atacantes. Y veremos también el primer ciberincidente en España en entorno industrial (o en algún operador de infraestructura crítica) con impacto en el ciudadano. La respuesta que se tenga ante este incidente (tanto a nivel de la propia compañía, como del sector o incluso gubernamental) será definitoria de todo el trabajo preventivo realizado hasta el momento en el sector.

Por si acaso, recomiendo tener a mano un buen servicio de seguridad gestionada con capacidad de detección y respuesta a incidentes".

## GyD IBÉRICA

**David González**

Director de Instituciones Financieras y Seguridad Empresarial OEM

"En 2017, la digitalización industrial continuará incrementándose de manera global proporcionando ventajas incuestionables, tales como la reducción de los costes de producción, debido a la optimización del rendimiento de la máquinas por un mejor aprovechamiento de las mismas. Sin embargo, con el aumento de la conectividad de las máquinas, el riesgo de espionaje industrial y de ciberataques crecerá rápidamente y cada vez con una mayor sofisticación y con el agravante de que los sistemas operativos de las maquinas industriales son de difícil actualización. Desde GyD nos enfocamos en desarrollar e implantar soluciones que permiten la conexión remota, de una manera segura e identificando cada máquina y cada usuario que accede a ellas".

## HP Enterprise

**Juan Navarro**

Sales Specialist. HPE Security Products

"Predecir la aparición de nuevos vectores o técnicas de ataque es una tarea cuanto menos atrevida: puede ser evolutivas o nuevas derivadas del descubrimiento de nuevas vulnerabilidades en aplicaciones, sistemas o comunicaciones; y aquí podemos incluir la asociadas a las provenientes del IoT. Es de entender la preocupación de las amenazas que están por venir, pero no podemos olvidarnos de las que ya conocemos: ya en el HPE CyberRisk Report de este año indicábamos que de las 10 vulnerabilidades más explotadas durante el último año, 6 eran conocidas desde el año 2009 y 2010, y alguna incluso tenía publicados dos parches de resolución. En cualquier caso, lo que las tendencias nos indican no es tanto el origen de la amenaza como el objetivo de la misma: el dato, bien para extraerlo ("monetización", aunque sea más apropiado llamarlo "tráfico"), modificarlo (fraude) y/o eliminarlo. No ha habido semana en este último año en que no se haya publicado en los medios alguna noticia relacionada con robos de información, y esto puede dispararse este nuevo año, y sobre todo de cara al 2018 cuando además las entidades que no hayan puesto en marcha medidas efectivas de protección de datos, se vean obligados a hacerlos públicos, tal como establece GDPR".

## IBERLAYER

**Pedro David Marco**

Fundador y CEO

"El ransomware ya ha demostrado su devastadora efectividad durante los pasados 2 años y medio. Los grupos organizados de ciberdelincuencia ya saben muy bien cómo llegar al usuario final (por correo electrónico en el 90% de los casos), engañarle y extorsionarle, por lo que ya sólo queda aumentar la rentabilidad... en lugar de cifrar ficheros y pedir rescate por ellos, se extraerán documentos privados y se amenazará con hacerlos públicos si no se paga, y no solo documentos... se extraerán licencias, claves personales, listas de contactos, historiales de navegación, etc., que además del problema obvio e inmediato que genera, con el GDPR el problema se convertirá en exponencial".

## IBM

**Jesús Romero**
Director de IBM Security para España, Portugal, Grecia e Israel

"En 2017 asistiremos a un incremento de las campañas de ciberataques esponsorizadas por gobiernos o por grupos criminales, y orientadas al ciberespionaje y/o al sabotaje, buena parte de esas campañas tendrán las IC como objetivo. Asistiremos a nuevas denegaciones de grandes servicios y *sites* de Internet por ataques distribuidos y aparecerá *ransomware* específico para el control y secuestro de los componentes de IoT. Por otro lado, buena parte del volumen total de ciberataques seguirá estando basado en vectores de ataque ya antiguos o ampliamente conocidos. En el lado de la ciberseguridad el hito tecnológico del año será la irrupción de la seguridad cognitiva, que mejorará de forma drástica las capacidades de las organizaciones en la detección y respuesta a los ciberataques".

## IMPERVA

**Jesús Vega**
Director Regional para Iberia

"Esperamos que el *hacking* prevalezca aún más en 2017, especialmente, debido a que es más fácil y barato que nunca, desde el acceso y alquiler de una amplia variedad de ataques desde *botnets*, hasta sofisticadas campañas de Phishing-as-a-Service. Adicionalmente, veremos que ataques "fantasma", como el de Yahoo en 2013 expuesto hace unos meses, continuarán apareciendo y sabremos de brechas importantes que ocurrieron en años anteriores. Asimismo, habrá un explosión de *botnets* y sus ejércitos crecerán en la medida que se aprovecharán de dispositivos inseguros, en particular dispositivos IoT baratos, que carecen de las adecuadas medidas de seguridad".

## INCIBE

**Alberto Hernández**
Director General

"Durante 2016 desde el CERT de Seguridad e Industria (www.certsi.es), operado por INCIBE bajo la coordinación de CNPIC e INCIBE, hemos gestionado más de 106.000 incidentes de ciberseguridad, de los cuales más de 450 han correspondido a operadores críticos de los diferentes sectores estratégicos (energía, sistema financiero, telecomunicaciones, etc.) y el resto al ámbito de ciudadanos y empresas (de toda índole y tamaño).
En este año los principales incidentes se han centrado en las infecciones por malware avanzado, destacando el ransomware, que por segundo año consecutivo se ha consolidado como la amenaza cibernética más destacada en ciudadanos y empresas por sus connotaciones de extorsión y chantaje. También han destacado el fraude electrónico, en sus diferentes modalidades, y los intentos de intrusión y accesos no autorizados a sistemas, redes e información. En cuanto a notificaciones, cabe destacar que durante el año 2016 desde el CERTSI hemos reportado más de 125 avisos de ciberseguridad a operadores críticos, más de 270 alertas de ciberseguridad para ciudadanos y empresas, más de 35 avisos relacionados con vulnerabilidades del tipo 0-day y, a través del servicio Antibotnet, se han enviado más de 30.000 notificaciones a los ISPs relativas a actividades maliciosas provenientes de redes de ordenadores zombi o botnets. Por todo ello, y de acuerdo con la experiencia de INCIBE, prevemos que durante 2017 y en relación a los ciudadanos y empresas, continuarán los ataques basados en malware destinados a la ex filtración de información y datos, las denegaciones de servicio con motivos políticos, geográficos o empresariales, el hacktivismo social y nuevos ciberataques a operadores críticos, probablemente utilizando nuevas tecnologías o tendencias como es el IoT y que hemos podido ver ya durante 2015 y 2016. En la otra cara de la moneda, las empresas seguirán invirtiendo al alza en ciberseguridad, adquiriendo nuevas capacidades destinadas a la detección y prevención de ataques, pero también a la mitigación de los mismos, reforzando también la capacitación y especialización de sus equipos humanos y tecnológicos. INCIBE por su parte seguirá apoyando como siempre el desarrollo de la ciberseguridad dentro de la Sociedad de la Información a través de sus servicios públicos gratuitos en ciberseguridad, www.incibe.es, www.certsi.es y www.osi.es".

## INNOTEC – GRUPO ENTELGY

**Félix Muñoz**
Director General

"Dado el éxito y la repercusión obtenida, los atacantes seguirán incrementado el número e intensidad de sus acciones con tres objetivos claros: información valiosa, dinero e interrupción de servicios, sea cual sea la superficie de ataque (ordenador, dispositivo móvil, Internet de las Cosas, redes sociales, etc.) o el método empleado (ransomware, ataques dirigidos, suplantación de identidad, etc). En esta situación, es el momento de pasar a una defensa más activa, poniéndonos en la mentalidad del atacante (equipos Red Team que evalúen todos los riesgos de intrusión, físicos y digitales), intercambiando conocimiento y ciberinteligencia y monitorizando las redes, equipos y sistemas para prevenir y detectar de forma rápida cualquier intrusión. En definitiva, tener la capacidad de evolucionar al ritmo de los atacantes e, incluso, anticiparse a sus acciones".

## INGRAM MICRO

**Antonio Anchustegui**
Business Manager Virtualization, Security & Networking

"Vemos cada vez más comprometida la seguridad de dispositivos móviles, Android y también iOS, con *jailbreak* o sin él. IoT seguirá siendo un objetivo prefe-

rente por el crecimiento del parque instalado y la pobreza de las políticas de seguridad aplicadas. Los sitios web serán atacados para acceder a los usuarios que se conecten, debido a la no aplicación exhaustiva de parches de seguridad. Los *plugin* muchas veces serán el objeto del ataque a estos sitios. En Ingenieria Social, lo más relevante seguirá siendo el timo del Servicio Técnico y el *malvertising*. La seguridad en el comercio clectrónico, por el momento, parece estar siendo bastante efectiva. El *phishing* es probable que decaiga. Y los ataques dirigidos y *time zero*, de *ransomware* o *data breach* seguirán siendo la principal amenaza a empresas e instituciones".

## INTERNET SECURITY AUDITORS

**Daniel Fernández**
Director Comercial

"Sin duda 2016 acabó con dos eventos que van a marcar si no este año, los siguientes: por un lado, lo sucedido en Estados Unidos y la supuesta injerencia de un gobierno extranjero, sumando la capacidad de manipulación de parte de la sociedad a través de las redes sociales mediante la publicación de informaciones generadas con ese fin y el hecho de que la falta de seguridad para acceder a información sensible pueda ser precisamente con fines de manipulación; por otro lado, el hecho que el IoT ya ha supuesto un problema de seguridad de tal magnitud que ha demostrado que la fiebre incontrolada e impulsiva por el "always connected" sin tener presente las implicaciones de seguridad que ello implica, van a ser un problema para la propia sociedad. Sociedad y seguridad están más ligadas y lo estarán más en un futuro".

## ISDEFE

**Óscar Pastor Acosta**
Gerente de Seguridad

"Si nos atenemos a lo ocurrido durante 2016 para predecir lo que pasará en el 2017, creo que uno de las elementos más imprevistos y sorprendentes ha sido el uso masivo de las "cosas conectadas a Internet" para llevar a cabo ataques distribuidos de denegación de servicio (DDoS), como los que sufrieron KrebsOnSecurity, Dyn o la francesa OVH. En mi opinión, lo interesante del caso no es la magnitud del ataque (record, más de 1 Tbps) sino que el "Internet de las cosas", normalmente visto como víctima, dada su pavorosa vulnerabilidad, ahora se convierte en "cómplice" de los cibercriminales. Mucho me temo que dada la precaria situación de los sistemas de control conectados a Internet, y de la domótica on line en general, este precedente marque tendencia durante 2017 (y no solo en ciberataques DDoS). Habrá que pedir más responsabilidad a los fabricantes y propietarios de estos sistemas, por conectarlos sin la diligencia debida en su protección, lo que como hemos visto puede dañar de forma severa a terceros".

## ITS SECURITY

**Álvaro Fraile**
CEO

"Este año nos encontraremos con ataques más sofisticados, más inteligentes, automatizados por completo y llevados a cabo con *malware* con habilidades adaptables que simularán el comportamiento humano.Los *hacktivistas* buscarán objetivos de gran valor, como pueden ser las infraestructuras críticas de un país, buscando un mayor impacto con sus ciberataques. Las ciudades inteligentes, los edificios automatizados y sus sistemas de gestión serán objetivo de los *hackers*. Los dispositivos IoT conectados serán el principal vehículo para ataques de ransomware y permitirá alcanzar a muchísimas más víctimas. Los clientes serán atacados a través de la nube de los proveedores aprovechando los millones de dispositivos conectados. Los fabricantes de dispositivos tendrán que rendir cuentas sobre la seguridad de sus productos".

## JUNIPER NETWORKS

**José Fidel Tomás**
Sr. System Engineer - Iberia

"Para 2017, los ciberataques evolucionarán en la dirección de contraatacar las nuevas técnicas de detección basadas en "Machine Learning" y "Sandboxing". Entendemos que dichas técnicas de detección han de provocar que los ciberataques se vuelvan muchos más cautos a la hora de introducirse en una compañía e incorporarán nuevas técnicas de mutación y de evasión que combatan las nuevas capacidades de detección que se van introduciendo tanto en sistemas "onpremise" como en "cloud" para luego proceder a la siguiente fase de propagación lateral una vez dentro de la red. Por ello, la colaboración entre los distintos elementos que componen la red a nivel global, tanto propios como de terceros, para la detección como para la aplicación de políticas de mitigación de amenazas, será clave a la hora de combatir los ciberataques a partir de este año 2017 que comienza".

## KASPERSKY LAB

**Alfonso Ramírez**
Director General de Iberia

"Las amenazas a medida y desechables tendrán más protagonismo, dejando en evidencia la fragilidad de un mundo cada vez más conectado. Muchas infraestructuras críticas están conectadas a Internet y no siempre con la protección necesaria. Asimismo, pronosticamos un aumento del *ransomware*, del cibersabotaje y del ciberespionaje dirigido a móviles e IOT. También crecerá la "mercantilización" de los ciberataques financieros con recursos especializados".

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?

## KPMG

**Javier Santos**
Director de Cibeseguridad. IT Advisory

"A partir de la información de control de la red de KPMG, los ciberataques durante 2017 estarán relacionados fundamentalmente con dos amenazas: en primer lugar en relación con los robos de información debidos a la fuga de datos en las organizaciones (sobre todo en los sectores de Retail and Consumer Goods, Entertaiment y Helthcare), lo que se está percibiendo ya por el volumen de noticias relativas a este problema (un 23% del total de noticias de ciberseguridad en las últimas semanas del 2016 y monitorizadas por nuestra red); en segundo lugar, nos encontraremos con un aumento en los ataques de DDOS sobrevenidos por las *botnets* soportadas por dispositivos IoT (elementos sin configuración de seguridad como sensores, CCTV o impresoras), de los que la *botnet* Mirai ha supuesto la punta de lanza. 2017 será el año en el que se verá una proliferación en la sensorización de sistemas derivados de la transformación digital de las organizaciones lo que supondrá una mayor vulnerabilidad frente a estas dos amenazas".

## LEET SECURITY

**Antonio Ramos**
Socio Director

"Es previsible que los ciberataques en 2017 vean un incremento de los ataques dirigidos. No podemos obviar la realidad: El escenario actual ya no tiene vuelta atrás y los atacantes van a seguir buscando la forma de realizar beneficios a través de la inseguridad de sus objetivos. En particular, una tendencia que estamos viendo desde LEET Security es el incremento de los ataques utilizando terceros como vías de ataque, o vulnerando a terceros que custodien la información de los objetivos. Es decir, la seguridad de la cadena de suministro va a ser un área en la que las organizaciones van a tener que incrementar su dedicación".

## LIDERA

**Antonio Camacho**
Product Manager

"Según los estudios de los distintos fabricantes que representamos en materia de ciberseguridad, donde más evolucionaran los ciberataques serán en los móviles;cada vez estarán más presentes los ataques de ransomware asociados a estos dispositivos. Aunque estos dispositivos suelen tener una copia de seguridad en la nube y esto reduce las posibilidades de pagar un rescate, creemos que los creadores de *ransomware* combinaran técnicas típicas de bloqueo asociadas al *ransomware*, con otros tipos de ataque asociados al robo de credenciales con el fin de acceder a cuentas bancarias y tarjetas de crédito".

## LOGALTY

**José Manuel Oliva**
Director General

"El ya acabado 2016 ha sido un año muy relevante en el ámbito de nuevas fórmulas para la contratación electrónica. La extensión de la segunda generación de la tecnología de cadenas de bloques (blockchain) hasta convertirse en un sustrato computacional operativo ha permitido la aparición de lenguajes especializados para transacciones electrónicas sin intermediarios clásicos, siendo especialmente notables aplicaciones como los Smart Contracts. Aunque estas tecnologías son ciertamente prometedoras, anticipamos la aparición de ciberataques a los mismos, de diversa tipología y gravedad, incluyendo significativamente ataques de denegación de servicio (en redes públicas), pero también afectaciones a la trazabilidad e identidad subyacente a las transacciones, como por ejemplo en caso de extracción o copiado de claves, que podrían afectar negativamente a la credibilidad del sistema; y por supuesto, prevemos la aparición de fraude basado en aplicaciones maliciosas que generan contratos ilegítimos, asegurándolos con este sistema, por lo que el papel del tercero interpuesto en el momento de la puesta a disposición continúa siendo imprescindible".

## LOGICALIS

**José Manuel Medina**
Director del área de Seguridad

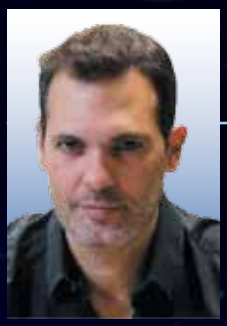
"Las organizaciones siguen centrándose en evolucionar las diferentes capas de seguridad más tradicionales (Perímetro y Data Center), así como la evolución de éstas hacia las redes definidas por software. Por este motivo, es plausible que los nuevos ataques de *malware* moderno se centren en ámbitos donde la seguridad "a priori" es menos madura, como pueden ser el Cloud, redes OT, o la Infraestructura de protección del IoT. Por ello es de prever que los nuevos vectores de ataque se focalizarán más en el "usuario", que sigue siendo el eslabón más débil de la ciberseguridad, y se hace necesario incluir nuevas herramientas de inteligencia cognitiva que proporcionen una capa adicional de seguridad. Un enorme facilitador para la protección contra ciberataques en 2017 será la adopción por parte de las organizaciones de la normativa europea de protección de datos personales (GDPR). Su obligado cumplimiento implica la implementación de medidas de seguridad que dificultarán enormemente a los ciberatacantes de su objetivo final, el DATO".

## LOGRHYTHM

**Rafael Esteban**
Southern Europe Sales Manager

"Hay diferentes vectores que amenazan con hacer de 2017 un mal año en términos de seguridad; las mafias han encontrado un filón y no lo van a soltar, la situación política en los principales países ha desatado una guerra subterránea donde la información es la nueva tierra a conquistar y precisamente esta situación política hace que los grupos independientes aumenten su actividad. Por desgracia, ransomware, DDoS o 0 days serán el pan nuestro de cada día y los paradigmas de la seguridad deben evolucionar porque la defensa perimetral se ha mostrado insuficiente".

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?



## LOGTRUST

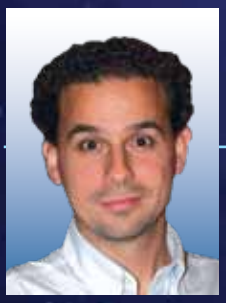
**Pedro Castillo**
CEO y Fundador

"En 2017 asistiremos a una nueva ola de amenazas avanzadas que tendrá como objetivo dispositivos IoT no *securizados* o no apropiadamente *securizados*. Las soluciones actuales de seguridad ya se han mostrado insuficientes para proteger frente a ataques IoT iniciados desde productos de consumo comprometidos, equipos médicos y sistemas embebidos entre otros. El riesgo que presentan los dispositivos IoT, con su rápido crecimiento, en breve excederá al existente en toda la base instalada de computación actual.Logtrust está en una situación inigualable para ofrecer las prestaciones, la estabilidad y la visibilidad necesaria para identificar y securizar dispositivos IoT".

## MCAFEE (INTEL SECURITY)

**María Campos**
Regional Director Iberia

"El ransomware ha sido el gran protagonista del 2016. Sin embargo, disminuirá en cantidad y efectividad durante la segunda mitad del 2017. Otras tendencias que serán noticia el próximo año son la "troyanización" de aplicaciones legítimas, el malware de IoT en la casa conectada y la aparición de ataques más sofisticados por parte de los cibercriminales. En 2017, será fundamental hacer un mayor uso de los análisis predictivos, mejorar la visibilidad tanto de los activos empresariales como de los datos descentralizados y reducir el número de agentes dedicados".



## MICROFOCUS

**Enrique Ramos**
Responsable de Identidad, Acceso y Seguridad para España

"En 2017, seguiremos viendo más de lo mismo en términos de vectores de ataque como *spearphishing*, *payloads* y *malware*. Serán cada vez más sofisticados, para asegurar que su éxito se mantiene, lo que implicará una mayor preparación y cuidado con el *phishing* inicial, y *malware* con más inteligencia para poder identificar cosas como redes de *honeypot,* análisis de memoria para identificar software de seguridad, etc. Asimismo veremos un mayor número de ciberataques publicados, no necesariamente porque el número aumente, sino como resultado de que las organizaciones comienzan a prepararse para el GDPR y mejorarán su seguridad en sistemas y procesos de gestión. Por último, veremos más ataques centrados en dispositivos IOT como resultado de que los fabricantes de estos dispositivos no están tomando la seguridad en serio, y que tendrán que aceptar que aunque el aumento de la seguridad tiene un coste para la usabilidad global, podría llegar a ser un diferenciador competitivo".

## MDTEL (SECUNIT)

**Francisco Cuesta**
Director de la Unidad de Seguridad

"IoT será una de los nuevos vectores de ataque tanto en su versión DDoS como de secuestro de dispositivos. Ransomware seguirá siendo una de las amenazas más relevantes para este nuevo año gracias la industrialización ofrecida mediante el uso de *frameworks* abiertos. Los gobiernos pasarán de mantener un papel más defensivo u oculto en el ciberespionaje a llevarlo a un plano de confrontación más claro y abierto afectando a organismos estatales y empresas privadas conectadas con estos. Otro de los vectores será la explotación de servicios *cloud* que usan de forma personal empleados (Shadow IT) y que ponen en riesgo la seguridad de la información".

## MICROSOFT IBÉRICA

**Héctor Sánchez Montenegro**
National Technology Officer

"Con toda Seguridad veremos un aumento de las amenazas a los dispositivos y endpoints, no solo los ya tradicionales ransomware, sino incluyendo aquellos elementos responsables del IoT. La superficie de ataque es enorme, y su protección continúa sin ser en absoluto suficiente. Asistiremos igualmente a una mayor conversación en el ámbito de la regulación al respecto, especialmente en Europa (NIS, GDPR) y finalmente asistiremos a una mayor demanda de automatización en la prevención, detección y respuesta a incidentes, especialmente a través de servicios basados en Cloud, que nos permitirán una respuesta avanzada que combine la IA, el BidData, el análisis (de datos y comportamientos) con aquellos otros elementos más habituales del mundo de la ciberseguridad".

## MINSAIT

**Manuel Escalante**
Director de Ciberseguridad

"El conjunto de incidentes acaecidos durante 2016 anticipa la evolución futura de los ciberataques en 2017. Seguirán evolucionando los vectores de ataque basados en dispositivos IoT y wearables, tanto como foco final como plataforma para otros ataques, y esperamos que sigan aumentando la utilización de ingeniería social como complemento a la sofisticación de ataques. Mención especial merecerán los dispositivos móviles, donde es previsible un incremento como plataforma de fraude; los incidentes sobre sistemas embarcados, como automóviles, aviones, etc., y los incidentes sobre sistemas en cloud centrados en explotar la relajación en la implementación de las políticas de seguridad de dichos entornos. Desde un punto de vista de defensa nacional, prevemos un incremento en los ataques contra infraestructuras críticas desde terceros países, como continuación de la tendencia de 2016".

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?

## NEOVALIA (GTI)

**Fernando Solabre**
Director

"La proactividad en la detección de vulnerabilidades y ataques en los dispositivos tradicionales, cada vez más protegidos, desviarán los ciberataques a dispositivos de más reciente implantación que están creciendo de forma masiva en nuestro uso cotidiano y cuya capacidad de proporcionarles protección es compleja por su variedad y el número incontrolado de ellos. Véanse los dispositivos IOT, *wereables* y otros elementos conectados que abrirán millones de puertas a ataques a capas superiores. Por otro lado, la ciberseguridad industrial va a ser un elemento en el que se va a tener que poner máxima atención y habrá importante crecimiento, ante la necesidad de proteger entornos de repercusión masiva a los ciudadanos y a sus centros económicos".

## NEXTEL, S.A.

**Juantxu Mateos**
Director de Desarrollo de Negocio

"Si a la impredecibilidad del ser humano y la disminución entrópica de la información, favorecida por la mejora de la calidad del dato, añadimos la incorporación exponencial de nuevos elementos a una red ya compleja de por sí, el resultado es una progresión de riesgos y brechas de seguridad no gestionados. Nos encontramos ante un terreno abonado para el natural desarrollo del cibercrimen, que dará un salto cuántico debido a su avidez por monetizar cualquier tipo de dato interesante para terceros. En este sentido, la maduración de su "modelo de negocio" conllevará a un entramado más complejo de socios, colaboradores y mercado objetivo, cuyo interés catalizará la diversificación de dicha actividad".

## ONE eSECURITY / SANS INSTITUTE

**Jess García**
Director de One eSecurity
Instructor Principal SANS

"Al no haber encontrado soluciones eficaces a los ataques que han plagado 2016, 2017 será seguramente un año de continuidad en su tipo (ransomware y Secuestro Manual de Datos, IoT DDoS, malware sofisticado y móvil, ciberespionaje, etc.), con un aumento en su superficie de ataque (cloud), frecuencia, intensidad y sofisticación. Se incrementarán los ataques con impacto en el mundo físico, y la infraestructura crítica será el campo de batalla civil en la nueva "Guerra Fría" entre estados (con cada vez más participantes). Las organizaciones deben hacer énfasis en estrategias reactivo-proactivas (Ciberinteligencia, Threat Hunting, Monitorización Continua, Respuesta a Incidentes) que permitan detectar e interrumpir los ataques antes de que su impacto sea crítico, y transferir parcialmente el riesgo a través de la contratación de Ciberseguros".

## ONESEQ (ALHAMBRA-EIDOS)

**José María Ochoa**
Director de Estrategia Corporativa

"Entrando en este prometedor 2017 que esperemos que sea el despertar completo de la empresas españolas en lo que se refiere a seguridad IT, desde OneseQ creemos que los ataques cada vez serán más dirigidos; el ransomware indiscriminado va a dar paso a una ataque con mayor capacidad de ingeniería social pero lejos de olvidarse de efectos masivos, también comenzará a actuar lo que se denomina Ransomware de las Cosas (RoT). Contra todo esto, las cinco claves que siempre aconsejamos: identificar, proteger, detectar, responder y recuperar… Sin visibilidad no controlaremos el riesgo".

## PANDA SECURITY

**Rosa Díaz**
Directora General de Panda Security España

"Las empresas sufrirán más ataques y cada vez más avanzados. Los ciberdelincuentes están continuamente buscando puntos débiles para entrar en las redes corporativas, y una vez dentro utilizan movimientos laterales para acceder a la información que buscan para robarla. Además, el ransomware, gran protagonista de 2016, lo seguirá siendo a lo largo de 2017, junto con los ataques DDoS. También hay que resaltar que vivimos un momento muy delicado en las relaciones internacionales. Diferentes amenazas de guerras comerciales, espionaje, arancelarias que pueden tener grandes –y graves– efectos en el campo de la seguridad informática pudiendo entorpecer las iniciativas existentes de compartición de información con estándares y protocolos de actuación internacionales. A nivel individual, el IoT es la próxima pesadilla de seguridad, ya que estos dispositivos no han sido diseñados con la seguridad como punto fuerte; y los móviles, donde los dispositivos Android se llevan la peor parte".

## PALO ALTO NETWORKS

**Tony Hadzima**
Director General para España y Portugal

"Los atacantes continuarán haciendo evolucionar sus mecanismos para monetizarlos al máximo. Así, veremos nuevos tipos de extorsión, como el Doxware, en el que se chantajea al usuario amenazándole con hacer pública información sensible si no paga (fotos, mensajes privados...). Por otro lado, habrá un incremento sustancial en las brechas de seguridad sobre servicios ofrecidos desde los grandes proveedores *cloud*, debido a la expansión que este tipo de infraestructura tiene. En cuanto a la evolución de las contramedidas, pensamos que la Inteligencia Artificial va a marcar el desarrollo de nuevos mecanismos de protección autónomos. Finalmente, y en lo que a regulación se refiere, en Europa la agenda estará marcada por la adaptación de los mecanismos de seguridad a las nuevas directivas NIS y GDPR de cara al 2018".

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?

## PROSEGUR

**Isaac Gutiérrez**
Director Global de Ciberseguridad

"Uno de los factores a los que hay que poner foco son las brechas en IoT, y especialmente en el ámbito industrial. Apostamos por un modelo de seguridad integral que, ante la capacidad de innovación de los *hackers*, permita a las empresas protegerse de manera adecuada. Particularmente en el ámbito de las infraestructuras críticas donde un ataque podría provocar daños realmente graves. Precisamente por el impulso del IoT entendemos que ahora mismo es prioritario actuar en la frontera cada vez más difusa que separa los mundos físico y digital. Un contexto donde, no olvidemos, nuestra privacidad y nuestros datos van a seguir siendo uno de los principales objetos de deseo para los ciberdelincuentes".

## PWC

**Javier Urtiaga**
Socio Responsable de Ciberseguridad

"Todavía hoy existe información muy limitada de los ataques recibidos y/o materializados por parte de las organizaciones. Si bien observamos tendencias de disminución de incidentes (como detalla la encuesta de Ciberseguridad que PwC efectúa a nivel mundial), es igualmente cierto que las compañías no disponen de la suficiente madurez en los sistemas de detección que avalen esta percepción. Y sin embargo, tanto la sensación de impunidad global de los adversarios, como el crecimiento exponencial de la superficie de exposición (número de dispositivos conectados, ya sea componentes de un *cloud*, dispositivos de usuario, IT, OT, etc.), nos lleva a pensar que los ataques seguirán aumentando en 2017. Por lo tanto, el reto para este año se focalizará en nuestra capacidad de modelar, anticipar y contener aquellas amenazas y vectores de ataque que por su impacto y repercusión, sí que debemos contemplar".

## RANDED

**Francisco Moral**
CMO

"Los métodos actuales basados en técnicas heurísticas y analíticas están dejando de ser eficaces porque la delincuencia organizada está utilizando técnicas de *machine learning* (Inteligencia Artificial) para mejorar de manera constante sus técnicas de ataque. Las técnicas de defensa deben pasar obligatoriamente por generar un mayor nivel de aislamiento frente los atacantes e incorporar mecanismos de machine learning a los procesos de monitorización y posteriormente a los de protección".

## RADIANTLOGIC

**Javier Franganillo**
Sales Manager

"Sin duda el nuevo año 2017 nos traerá más ciberataques cada vez más complejos y desde más frentes. La transformación digital, la movilidad y el internet de las cosas, deparan más vulnerabilidades que requieren de nuevos planteamientos para nuevos retos, en ese contexto consideramos que la identidad se configura como elemento central para mitigar esos riesgos.
Disponer de un perfil enriquecido de nuestros empleados, socios, clientes y todo aquel que accede a nuestros sistemas, nos facilitaran el identificar posibles vulnerabilidades. No sirve el planteamiento tradicional de gestión de identidad de nuestros empleados (LDAP, AD), tenemos que poder unificar todos los atributos que podamos recolectar (BBDD, etc.) con independencia de donde residan estos, para garantizar que la persona o cosa que accede sea quién dice ser y que accede a los recursos adecuados. Es lo que desde RadiantLogic llamamos Federación de Identidades".

## ROOTED CON

**Omar Bembouzza Villa**
Co-organizador

"Siguiendo la estela que nos dejó el pasado año, los "malos" se centrarán en obtener dinero de manera fácil y rápida mediante el fraude y la extorsión, tanto a usuarios como a empresas, véase los famosos ataques de "scam" de servicios técnicos, el denominado "fraude del CEO" así como el Ransomware. La evidente debilidad de los dispositivos IoT incrementará los daños y sabotajes a organizaciones cuyos dispositivos están conectados".

## RSA

**Fidel Pérez**
Responsable de Ventas para España y Portugal

"Adivinar el futuro no es una tarea trivial, pero basándonos en la experiencia de los últimos años seguro que vamos a ver ataques a infraestructuras críticas, redes IoT, ataques DDoS, aumento del ransomware... Sin duda todo ello es importante, pero desde el punto de vista de la empresa creemos que es mucho más importante analizar esa evolución de los ciberataques, con un conocimiento riguroso de la posición de riesgo de los activos críticos de la compañía y la preparación de la misma para reaccionar ante los de mayor impacto. Desde esta perspectiva creemos que las APTs dirigidas y especificas buscando la exfiltración de datos de propiedad intelectual o de información de clientes ocuparán los primeros puestos en los ciberataques que veremos en 2017 y que sin duda serán los más perjudiciales".

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?

## SAFELAYER

**Francisco Jordán**
Director General

"El robo de información privada en general y de identidad en particular seguirá teniendo un papel destacado en el catálogo de ciberataques. La transformación digital a través de la nube, la movilidad y la internet de las cosas está trasladando el fraude a las relaciones sin presencia física. Esto obliga a la ampliación del perímetro de prevención de amenazas empezando por aumentar la fortaleza, y la usabilidad, de la autenticación de usuarios y dispositivos".

## S2 GRUPO

**Antonio Villalón**
Director de Seguridad

"Durante 2017 veremos más ataques relacionados con IoT, tanto como origen del ataque (ejemplo: DDoS) como objetivo del mismo (dispositivos ICS, dispositivos médicos, etc.). Los ataques que impliquen beneficio económico para el atacante también se incrementarán, desde nuevos modelos de "negocio" basados en ransomware como ataques tipo CFO, compra y alquiler de capacidades, etc. Finalmente, en los ámbitos ligados al robo de información creemos que la actividad se mantendrá, aunque sí es cierto que cada vez salen a la luz víctimas de más peso (ejemplo: DNC) y con motivaciones no solo geopolíticas, sino también económicas detrás (ejemplo: Yahoo)".

## SECURE&IT

**Francisco Valencia**
Director General

"En 2017 vamos a ver un gran aumento de las APT, que van a ir dirigidas sobre todo a industria. Los cibercriminales se han dado cuenta de que los entornos industriales son fácilmente atacables debido a su obsolescencia tecnológica. Se han adaptado redes de nueva generación a sistemas muy antiguos, que son tremendamente vulnerables. Además, es muy difícil protegerlos porque la actualización es complicada".

## SAILPOINT

**Javier Drake**
Director de Ventas para España y Portugal

"Desde SailPoint vemos que habrá un movimiento hacia la seguridad del comportamiento, ya que las empresas se están dirigiendo a este modelo conductual; es el motivo por el cual el contexto de la identidad en la Gestión de Identidades y Accesos es tan importante. Es el centro de todo lo que hacemos. Con esto, la Gestión de Identidades y Accesos será un requisito para todos, tanto para empresas grandes como pequeñas. Adicionalmente, habrá un foco importante en los datos no estructurados."

## SECUTATIS

**Ángel Fernández**
Director de Ventas y Desarrollo de Negocio

"Sin duda los focos principales de las ciberamenazas van a estar centrados en el IoT, la Cloud, la Movilidad, las Infraestructuras Críticas y en general en todo tipo de entornos empresariales y personales donde residen múltiples datos sensibles susceptibles de ser comercializados por los ciberdelincuentes, luego hay que adoptar una estrategia contundente para protegerlos. Las fugas de información de carácter empresarial y personal serán mucho más graves y habrá que abordar urgentemente una hoja de ruta para adaptarse al cumplimiento del Reglamento Europeo de Protección de Datos (GDPR) ya en vigor antes de que el periodo de adaptación finalice en mayo del 2018 mediante la adaptación o revisión de tecnologías, procesos, políticas y controles como la ofuscación, la clasificación, el cifrado de la información y otros con el objetivo de proteger la misma con independencia de su ubicación".

## SONICWALL

**Nicasio de Tomás**
Director de Canal Iberia

"Los tipos de ransomware van a evolucionar para evitar ser detectados por sistemas de tipo *sandboxing* y otros y se van a extender a hogares y *smartphones*. En cuanto a IoT, ya existen PoCs y demos en las que se han comprometido *smart*TVs, frigoríficos, coches y hasta sillas de ruedas, su compromiso afectará sobre todo a los ataques DDoS y posiblemente a ransomware. Respecto a ataques DDoS serán cada vez más masivos y a gran escala gestionados por *botnets* sobre todo basadas en IoT. En lo relativo a ataques a la nube, como la información está centralizada son objetivos muy atractivos para los atacantes (ataques de tipo DDoS masivos y robo de datos). Respecto a ataques a infraestructuras críticas (SCADA), como este tipo de infraestructuras son un objetivo común en la ciberguerra, seguirán siendo una tendencia creciente".

## SERVICENOW

**Joaquín Reixa**
Vicepresidente para el Sur de Europa

"En 2017 los ciberataques continuarán creciendo en complejidad, y al mismo tiempo las herramientas necesarias para su despliegue estarán disponibles más fácilmente para los cibercriminales. Ya en 2016 pudimos ver herramientas

de "Ramsomware-as-a-Service" (RaaS) para realizar ataques DDoS. Las soluciones para prevención y detección son el primer paso para la protección. No obstante, lo que realmente precisa una organización es un Programa de Respuesta de Seguridad combinado con una aproximación de gestión de una CMDB para toda la organización, que incluya también los dispositivos "wearables" y objetos conectados, permitiendo a las organizaciones responder y resolver las amenazas más importantes con rapidez. Y esta situación se verá incrementada al calor del crecimiento de los dispositivos conectados IoT. En 2016 observamos una serie de ataques DDoS masivos desde *botnets*IoT, por lo tanto las empresas deben tener muy en cuenta la seguridad en sus diseños de estrategias IoT".

## SPAMINA

**Enrico Raggini**
Presidente y CEO

"El crecimiento de las ciberamenazas está asociado al uso de nuevas tecnologías en el ámbito de la comunicación empresarial. Si bien el email continua siendo el principal puerto de acceso, donde los ataques 'targetizados' son cada vez más difíciles de detectar; la mensajería instantánea se ha implantado de forma regular en las compañías sin tener en cuenta que el uso de herramientas de consumo particular no cuentan con seguridad integrada. Esto permite a los ciberdelincuentes acceder a la información de los dispositivos móviles y, además, una difusión masiva en tiempo real".

## STORMSHIELD

**Antonio Martínez Algora**
Responsable Técnico en Iberia

"El mercado del ransomware seguirá creciendo y afectando tanto a particulares como a empresas de cualquier tamaño y sector. Continuará mutando y volviéndose más peligroso: Si hasta ahora la técnica mayoritaria precisaba de la participación del usuario mediante la apertura de adjuntos recibidos por correo, se consolidarán nuevas herramientas específicas, tales como kits de "Ramsomware-as-a-Service" (RaaS) que permiten a un grupo de ciberdelincuencia "revender" sus ataques y al uso de vulnerabilidades de Día Cero o *exploits,* que no requieren de la participación activa del usuario. La confluencia del mercado de *exploits* y del ransomware generará variantes más peligrosas aprovechando la extensión a nuevos sistemas operativos y a infraestructuras críticas, aprovechando la fragilidad de los sistemas de protección tradicionales que resultan fáciles de eludir".

## S21SEC

**Xabier Mitxelena**
Board Member & Founder

"Después del 'año del ransomware', que ha venido para quedarse, vamos a asistir a una "revolución" en los objetivos de los ataques y no tanto en los modelos/formatos. Los ataques a empresas de todo tipo y tamaño van a crecer de forma importante, y veremos aparecer nuevos Ciberdelincuentes "autónomos" e "individuales". Las APT's van a evolucionar siguiendo objetivos económicos y políticos, con especial énfasis en Infraestructuras Críticas, pero se espera una reducción del tiempo de infección de la Industria afectada. Además, las novedades tecnológicas serán el camino a través del cual buscar el éxito: Cloud, IoT y, sobre todo, *smartphones*".

## SVT CLOUD SECURITY

**Josep Bardallo**
Director

"Durante el 2017 consideramos que los ciberataques se van a incrementar principalmente por la vertiente más débil hoy día: las personas. Por lo tanto vamos a encontrarnos con un incremento de los ataques de ingeniería social, dirigidos y no dirigidos, con el objetivo de comprometer no solo la privacidad, sino además para incrementar la potencia de ataques posteriores (DDoS, ataques corporativos...) o como otro método más de cibercrimen (*ransomware*, etc.). Además, se va incrementar la superficie de ataque a las organizaciones, ciudades y los particulares, ya que los dispositivos IoT ya forman parte de los mismos, y los ciberdelincuentes se van aprovechar de su falta de seguridad en el diseño y las configuraciones por defecto que incluyen los fabricantes, así como su dificultad de incorporar actualizaciones de seguridad".

## SWIVEL SECURE

**Alex Rocha**
Director Regional

"Los avances tecnológicos en las TI siempre estarán acompañados del desarrollo de la delincuencia informática y cada vez más en sectores verticales motivados por razones financieras y políticas.Los paquetes de *exploits* fueron la tendencia en 2016 junto con el crecimiento exponencial de ransomware, phishing y malware, delitos cibernéticos que tenderán a aumentar y a difundirse. Por ejemplo, el ransomware persistirá con la adición de '*sextorsión*' donde los más afectados serán los niños.Por otro lado, continuarán los ataques a la Banca (FlokiBot es una de las mejoras de Zeus y ataques a la Banca de bitcoin), grandes corporaciones (YahooBreach, evoluciones del Stuxnet) y Gobiernos (elecciones en los EUA, NSA). Y, además, es posible que se inicien los primeros ataques a aviones y camio-

nes (hijacking), una nueva fuente para los terroristas. Con todo, en 2017, una de las tendencias más fuertes serán los sistemas de nubes virtualizados y los dispositivos móviles, así como la explotación de vulnerabilidades de IoT que permiten acceder a una red de dispositivos basados en códigos obsoletos".

## SYMANTEC
**Miguel Martos**
Country Manager para Iberia

"2017 será el año de la consolidación de un nuevo paradigma de la TI empresarial. Junto a la red corporativa sin perímetro, sin red WAN, se consolidarán las aplicaciones corporativas suministradas por proveedores SaaS, con aún mayor movilidad de usuarios utilizando dispositivos personales y corporativos, indistintamente, para hacer su trabajo, y con una parte significativa de centros de datos desplegados sobre proveedores IaaS. En este nuevo marco las empresas deberán centrarse en la protección de lo que serán realmente sus dos únicos activos de TI: la identidad y los datos.Del mismo modo el *malware* se adaptará a este nuevo escenario concentrando sus esfuerzos en el robo de identidades corporativas como medio directo del acceso a los datos almacenados en nubes públicas y privadas, y desarrollará nuevos mecanismos de propagación empleando esos mismos servicios SaaS corporativos".

## TARLOGIC
**Andrés Tarascó**
Fundador y CEO

"Las tendencias que identificamos desde Tarlogic Security para este 2017 van dirigidas y poniendo enfoque en el aumento de vulnerabilidades en entornos IoT, lo que se traduce en ataques masivos desde estos dispositivos a las grandes industrias; seguiremos observando los mismos objetos de riesgo que en años anteriores, que requerirán el esfuerzo de no perder el foco en lo tradicional, principalmente la lucha contra el cibercrimen 360, mobile exploiting, ataques dirigidos, así como la de mantener una visión pragmática para contrarrestar de forma efectiva (incluida la ofensiva) los riesgos -de todos los de tendencia y los de siempre-, con foco en la resilencia".

## THALES e-SECURITY
**Jordi García**
Ingeniero de Ventas para el sur de Europa

"El crecimiento exponencial del IoT está abriendo las puertas a nuevas tecnologías que están ya presentes o emergiendo, y debido a carencias de seguridad en su diseño, van a convertirse en nuevos vectores de ataques avanzados, aumentando así en forma y número los APT dirigidos que van a tratar de comprometer la integridad de negocio de entidades de todo tipo, ya sean empresas,instituciones financieras u organismos públicos".

## TREND MICRO
**José Battat**
Director General de Iberia

"Los ciberdelincuentes evolucionan a medida que lo hace la tecnología y, por eso, explorarán nuevas gamas y superficies de ataque. Las redes de *bots* en IoT causarán estragos DDoS, especialmente en sitios de servicios de noticias, corporativos y políticos; y tanto IoT como el IIoT tendrán un papel protagonista en los ataques dirigidos. Prevemos un alza de las estafas BEC entre el personal financiero, y un 25% más de nuevas familias de r*ansomware* con especial foco en los ataques a TPV, cajeros automáticos y sistemas industriales. La ciberpropaganda será una tendencia peligrosa, a pesar de no ser una ciberamenaza en sí para las empresas. Por su parte, las redes sociales seguirán siendo objeto de abusos y está por ver si la retirada de la publicidad de los sitios que publican historias falsas tendrá algún efecto".

## T-SYSTEMS IBERIA
**Laura Hernández Ardura**
Security Operations Manager

"Sin duda 2016 se ha marchado plagado de noticias y escándalos sobre ciberataques y fugas de información que han afectado incluso a campañas presidenciales. En consecuencia, no podemos más que esperar una tendencia alcista de los mismos para 2017, tanto en número, como en complejidad y/o impacto. Viviremos una "democratización" de los ciberataques que hará que aumente el número de ataques menos sofisticados llevados a cabo por actores noveles en estas lides que harán uso de las herramientas puestas a su disposición por otros más avanzados. Por otro lado, actores profesionalizados, auspiciados por gobiernos o grupos organizados criminales, desarrollarán ciberataques de mayor complejidad e impacto, explotando el filón de dispositivos IoT inseguros y plagados de vulnerabilidades, y explotando el eslabón más débil: el ser humano, mediante ataques sociales dirigidos. Hablando de complejidad e impacto no podemos dejar de señalar dos variables más: el uso del cifrado, y los proveedores de *cloud* pública como blanco claro de una interrupción masiva que afecte a múltiples clientes".

## VERISEC
**Anders Bahrton**
Director para España

"Las amenazas más importantes para este año se van a ver reflejadas en las áreas de mayor crecimiento en el mundo IT. Estas se

verán más expuestas a ataques. En 2017 veremos un aumento exponencial en el crecimiento del uso de APPs tanto para el sector privado como el profesional. Las empresas seguirán apostando cada vez más por las tecnologías que tengas presencia en la nube. Y por último veremos el crecimiento del Internet de las Cosas conectando nuestras vidas y hábitos con internet. En Verisec seguiremos manteniendo el foco en la gestión de identidades y la autenticación fuerte integrándonos cada vez más en las nuevas tecnologías. Otra área en el que nos enfocamos es en la seguridad de las APPs manteniendo la usabilidad. Verisec apuesta por alternativas para este año 2017 como puede ser la eliminación de los SMS para aprobación o validación".

**VINTEGRIS**
**Facundo Rojo**
Director General

"2017 será un año apasionante en cuanto a la aplicación de las tecnologías de la información en el ámbito de seguridad. El concepto "Internet de todas las Cosas, IoE (Internet of Everythings)", proporciona una superficie enorme de vulnerabilidades y aumenta de forma exponencial el riesgo, la seguridad es ya un punto clave de inflexión en la transformación digital y el adecuado tratamiento de la misma se va a transformar en "driver" en la economía del conocimiento. Tanto a nivel industrial (en máquinas e infraestructura) como a nivel individual (de las personas), el usuario seguirá siendo el principal punto de ataque, el ransomware es un método sencillo que permite actuar a los cibercriminales con muy poco esfuerzo. Oiremos con mayor frecuencia hablar de automatización en seguridad, existe una corriente de tecnología cognitiva que requiere de equipos (empresas y personas) altamente especializados en el manejo de datos desestructurados, que son el verdadero punto de inflexión competitivo en verticales de negocios sensibles como las áreas financieras, de salud o retail por citar algunas de entre otras, que deberán prestar atención y dedicar recursos a atender las necesidades de seguridad".

**V-VALLEY IBERIAN (antigua ITWAY)**
**David Tauste**
Director Comercial

"2017 se presenta con un alto nivel de ciberactividad. Se vislumbra un aumento significativo de la explotación de las vulnerabilidades de los dispositivos que se incorporan a la internet de las cosas, con el objetivo más que probable de ser origen de ataques a terceros. También veremos una intensificación de los ataques dirigidos a infraestructuras críticas, no solo de control industrial, sino también contra proveedores de servicios, aplicaciones, comunicaciones, infraestructuras en la nube... Y también se intensificará el acopio de credenciales y datos personales de usuarios de redes sociales, con el objetivo de ganar acceso a las aplicaciones de las compañías donde trabajan estos usuarios".

## VATICINIOS

**Las predicciones y aseveraciones expuestas a continuación son una muestra extraída de las respuestas dadas a la pregunta "¿Cómo van a evolucionar los ciberataques en 2017?" formulada por SIC. Las hay arriesgadas, conservadoras, tramposas, generales, detalladas, ocurrentes… Pero ninguna sin fundamento.**

- Explotación de vulnerabilidades de soluciones de gestión de APIs y entornos con contenedores de aplicaciones y microservicios.
- Multiplicación de botnets al servicio de ataques de DDoS contra protocolos y servicios no habituales: DNS, NTP…
- Crecimiento en el secuestro de servicios en la nube y en ataques a proveedores de servicios.
- Ataques dirigidos al engaño del usuario con el objeto de que el mismo cree una firma electrónica cualificada respecto a un contenido malicioso.
- Emergerá el "planting" como actividad de soborno a personal interno con mucha fuerza como elemento 'troyanizador' físico que permita el éxito de los ciberataques adicionalmente a las tácticas y técnicas vistas durante 2016.
- Las soluciones actuales de seguridad ya se han mostrado insuficientes para proteger frente a ataques IoT iniciados desde productos de consumo comprometidos, equipos médicos y sistemas embebidos, entre otros.
- Mayor frecuencia y agresividad de las infecciones y propagación del malware con foco en la extorsión, pudiendo afectar a todo tipo de plataformas y verticales: Smart cities, IoT, infraestructuras críticas, móviles, drones… Esto se verá dinamizado por la facilidad de cobro y movimiento de divisas a través de criptomonedas como bitcoin.
- Quizá veamos pasar del mero secuestro de los datos mediante cifrado, a la extracción de los mismos para amenazar con su publicación (Doxware).
- Posible nacimiento del "RamsomGDPRware", dirigido a grandes instituciones a las que se extorsionará ante la amenaza de la sanción y/o notificación".
- Ciberespionaje: se espera mayor variedad de ataques sobre plataformas móviles de personas clave en administraciones públicas y empresas estratégicas.
- La desaparición de los grandes exploit kits (Angler, Nuclear, Neutrino) creará nuevos grupos de ciberdelincuentes más pequeños, numerosos y focalizados.
- Incremento de los ataques a administradores de red y de sistemas.
- La delincuencia utilizará la nube para acelerar la producción de herramientas de ataque, que serán cada vez más robustas y difíciles de combatir.
- A medida que se consoliden las Fintech, aumentará el interés de algunos en atacar a los nuevos servicios financieros para beneficio económico propio.
- Se incrementarán las operaciones cibernéticas motivadas políticamente que, por lo general, rodean los conflictos globales o regionales (China, Rusia, ataques de los estados nacionales).
- Veremos el primer ciberincidente en España en entorno industrial (o en algún operador de infraestructura crítica) con impacto en el ciudadano.
- Continuarán apareciendo ataques "fantasma", como el de Yahoo en 2013 expuesto hace unos meses, y sabremos de brechas importantes que ocurrieron en años anteriores.
- Los fabricantes de dispositivos tendrán que rendir cuentas sobre la seguridad de sus productos.

# ¿CÓMO VAN A EVOLUCIONAR LOS ATAQUES EN 2017?

## VULNEX

**Simon Roses**
Fundador y CEO

"A raíz de la publicación del código de Mirai podemos esperar un año plagado de ataques a dispositivos IoT, inseguros por defecto. Malware en móviles y atacantes profesionales de Estado-Naciones afectarán a organizaciones y gobiernos del mundo entero que no establezcan unas medidas de seguridad mínimas".

## WATCHGUARD

**Guillermo Fernández**
Sales Engineerpara Iberia y PALOPs

"Para este 2017, las empresas continuarán siendo blanco del ransomware. Los atacantes son conscientes de la rentabilidad que les ha supuesto y por ello van a mejorarlos. Esperamos ver el primer *ransomworm*, con capacidades para infectar otros equipos de forma automática, y también mejoras en sus tácticas evasivas. También consideramos que, dado el uso cada vez mayor de los servicios IaaS, estos serán blancos de ataques y desde un proveedor IaaS esperamos ver un ataque relevante publicado en los medios".

- La "Internet de las cosas", normalmente vista como víctima, se convertirá en "cómplice" de los cibercriminales dada su pavorosa vulnerabilidad.
- Los ciberataques evolucionarán en la dirección de contraatacar las nuevas técnicas de detección basadas en "Machine Learning" y "Sandboxing".
- Crecerá la "mercantilización" de los ciberataques financieros con recursos especializados.
- Incremento de los ciberataques utilizando terceros como vías de ataque, o vulnerando a terceros que custodien la información de los objetivos.
- Asistiremos a la aparición de fraude basado en aplicaciones maliciosas que generan contratos ilegítimos.
- Veremos un aumento de las amenazas a los dispositivos y endpoints.
- Seguirán evolucionando los vectores de ataque basados en dispositivos IoT y wearables.
- Las APTs dirigidas y específicas buscando la exfiltración de datos de propiedad intelectual o de información de clientes ocuparán los primeros puestos en los ciberataques.
- Alza de las estafas BEC entre el personal financiero, y un 25% más de nuevas familias de ransomware con especial foco en los ataques a TPV, cajeros automáticos y sistemas industriales.
- Viviremos una "democratización" de los ciberataques, que hará que aumenten los menos sofisticados llevados a cabo por actores noveles en estas lides usando herramientas facilitadas por otros más avanzados.
- Se intensificará el acopio de credenciales y datos personales de usuarios de redes sociales, con el objetivo de ganar acceso a las aplicaciones de las compañías donde trabajan estos usuarios.

## VORMETRIC

**Ignacio Berrozpe**
Sales Engineer

"En 2017 observaremos una mayor visibilidad si cabe de ciberamenazas y ciberataques. Por un lado el entorno regulatorio y la inminente entrada en vigor del Reglamento General de Protección de Datos de la UE sensibilizará más al entorno de administraciones públicas y empresarial con la adopción de medidas que protejan la privacidad contra los ciberataques. Además esperamos un paso más en la escalada armamentística entre ciberataques y ciberdefensas, con la adopción de tecnologías basadas en la modelización estadística de código y comunicaciones para su detección temprana, aprendizaje automático ("machine learning") por parte de los elementos de defensa y tecnologías de reconocimiento de amenazas basadas en el análisis de grandes cantidades de datos históricos "big data". Finalmente en el ámbito de los estados naciones, las amenazas y los ataques seguirán previsiblemente al alza, con una incidencia especial en las infraestructuras críticas, ya sean militares o industriales".

## WESTCON SECURITY IBERIA

**Sergio Dombriz**
Director de Desarrollo de Negocio
de Soluciones de Seguridad

"La evolución de ciberataques en este 2017 afectará en cinco puntos: 1) Brechas de seguridad en las organizaciones debido a ataques en dispositivos móviles corporativos; 2) Interrupciones y robos de información en proveedores de servicios en la "nube" que afectarán a múltiples clientes; 3) Los "secuestros virtuales (ransomware)" se propagarán a las infraestructuras "Cloud"; 4) Millones de dispositivos hiperconectados sin seguridad básica, usados como fuerza de choque por los ciberdelincuentes (IoT), y 5) Se duplicarán los ataques a infraestructuras críticas y sistemas de producción".

## ZSCALER

**Michael Sutton**
Vicepresidente de Investigación en Seguridad

"Los cibercriminales van a seguir profesionalizándose y explorando nuevos métodos de ataque y extorsión. Se seguirá buscando inutilizar el hardware enfocándose también en dispositivos IoT. Se incrementarán las campañas de desprestigio de empresa, no sólo para recabar datos privados sino también alterando la información existente. El auge del *machine learning* será también aprovechado por los cibercriminales para lanzar ataques automáticos. Sin olvidarnos del aumento del uso de las redes sociales como medio para propagar ataques mediante *social networking bots*".