CCN-CERT
centro criptológico nacional

CIBERAMENAZAS Y TENDENCIAS 2018

CCN-CERT IA-09/18

RESUMEN EJECUTIVO

ÍNDICE

PRÓLOGO

1

El presente documento es un extracto del ***Informe de Amenazas y Tendencias.*** Edición 2018, publicado por décimo año consecutivo por la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (**CCN-CERT**). En él se realiza un análisis de las ciberamenazas, nacionales e internacionales, de su evolución y tendencias futuras. Buena parte de la información aquí recogida es el resultado de la experiencia del CERT Gubernamental Nacional que, en el año 2017, gestionó un total de 26.500 **ciberincidentes**, lo que supone un 26,55% más que en 2016.

El Centro Criptológico Nacional, en su actividad diaria, ha podido constatar que **los actores estatales y los criminales profesionales continúan siendo las amenazas más importantes,** al tiempo que la ciberguerra, los ciberconflictos y la **guerra híbrida** se hacen cada día más presentes en el mundo, siempre apoyados por acciones en el ciberespacio.

Por su parte, las **vulnerabilidades de dispositivos Internet of Things** (IoT, dispositivos cotidianos conectados a Internet) han propiciado ataques disruptivos que justifican la necesidad de mejorar la resiliencia digital.

Además, en 2017 se ha podido comprobar cómo a través de distintos ciberataques se ha intentado debilitar las democracias, interfiriendo en sus procesos electorales y alimentando sus conflictos internos.

Con el objetivo de afrontar los riesgos actuales, el documento matriz y el presente resumen ejecutivo analizan los **principales ciberincidentes de 2017**; los **métodos de ataque** empleados por los **agentes de la amenaza** contra sus víctimas; las múltiples **Vulnerabilidades** existentes que facilitan esta situación y las principales **medidas** a tener en cuenta con el fin de mejorar la seguridad.

Del mismo modo, y teniendo en cuenta la evolución de los ciberincidentes en el periodo considerado, se abordan algunas **tendencias** de cara a los próximos meses en los que es de esperar que los ciberataques incrementen su grado de sofisticación, de virulencia y de osadía.

El *Informe de Amenazas y Tendencias. Edición 2018* ha sido realizado con el propósito de resultar de utilidad para los responsables de seguridad TIC de las entidades públicas españolas, las organizaciones de interés estratégico y, en general, a los profesionales y ciudadanos de nuestro país.

2 CIBERINCIDENTES

En este epígrafe se desarrollan los ciberincidentes más significativos de 2017, agrupados por las motivaciones de los agentes de las amenazas.

CIBERCONFLICTOS

La sustracción digital, la publicación de información o la intoxicación de los medios de comunicación o las redes sociales se han utilizado estratégicamente por actores estatales para **desestabilizar a otros Estados y polarizar a la población civil.** Estos ataques se han llevado a cabo al amparo de procesos electorales o situaciones de conflicto.

Las **víctimas** de este tipo de operaciones han sido, en la mayoría de las ocasiones, **instituciones democráticas y partidos políticos** de diversos países, entre los que se encuentra España.

ACTIVIDADES DE INFLUENCIA

Estas actividades se basaron en la sustracción de información de partidos políticos y de sus miembros para influir en los procesos democráticos.

El partido político alemán, *Unión Democrática Cristiana (CDU); el movimiento En Marche!*, del presidente francés Emmanuel Macron; y los partidos Republicano y Demócrata de Estados Unidos fueron víctimas en 2017 de ciberataques de este tipo.

CIBERESPIONAJE

Esta problemática ha afectado durante 2017 a todos los países de nuestro entorno occidental. El ciberespionaje representa una amenaza que confirma el interés de los atacantes por obtener **información sensible** de las empresas e instituciones tanto españolas como occidentales.

DISRUPCIÓN DE SISTEMAS

La novedad en este tipo de ataques radica en el empleo de **dispositivos de Internet of Things (IoT)** de consumidores finales para perpetrar significativos ataques DDoS[1]. Así lo hicieron la botnet *Mirai* o la botnet *LizardStresser*, que infectaron decenas de miles de dispositivos de consumidores.

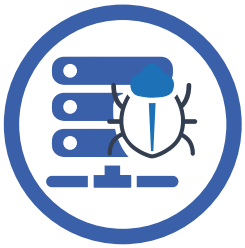
De la misma forma, las redes de energía eléctrica de Arabia Saudí, así como ciertas agencias gubernamentales también fueron víctimas de ciberataques en 2017, empleándose para ello el código dañino *Shamoon*.

OBTENCIÓN DE BENEFICIOS ECONÓMICOS

En 2017 también se llevaron a cabo ataques con el objetivo de obtener rendimiento económico. Para ello, se emplearon distintos métodos.

FRAUDE AL CEO

Los delincuentes intentan que el departamento financiero de una empresa realice transacciones económicas utilizando nombres de dominio similares al de la organización en cuestión.



MALWARE COBALT[2]

Envío de correos electrónicos a empleados de bancos con un archivo adjunto malicioso que permitía tener acceso a la red bancaria interna e infectar los servidores que controlan los cajeros automáticos.

CIBERPIRATERÍA

En Italia, la policía detuvo en 2017 a dos individuos sospechosos de ciberpiratería, que habrían realizado inversiones basándose en información robada.

1. DDoS (Distributed Denial of Service / Denegación de Servicio Distribuida): se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios prestados por él.
2. El líder del grupo cibercriminal, creador del malware Cobalt (2016-2018) fue detenido en España en marzo de 2018. Con este malware atacaron a más de 100 instituciones financieras de más de 40 países, generando pérdidas de mil millones de euros.

3 ACTORES DE LA AMENAZA

En este epígrafe van a examinarse los actores de la amenaza que, de forma intencionada, han desarrollado " o pretendido" ataques. Se prestará atención a la intención perseguida, a sus capacidades y a los cambios que se han observado.

LOS ESTADOS

Durante 2017, las agencias gubernamentales de muchos países del mundo, *-incluyendo España-* fueron repetidamente víctimas de persistentes ataques de ciberespionaje a gran escala, originados en terceros países.

Los Servicios de Inteligencia occidentales han identificado que **muchos países están invirtiendo en la creación de capacidades de ciberdefensa** (esencialmente ciberguerra o "guerra híbrida") destinadas al sabotaje de procesos críticos o dirigidas a influir en las operaciones de información.

Los métodos de ataque de los Estados son cada vez más sofisticados y, en consecuencia, más **difíciles de detectar.**

CIBERDELINCUENTES

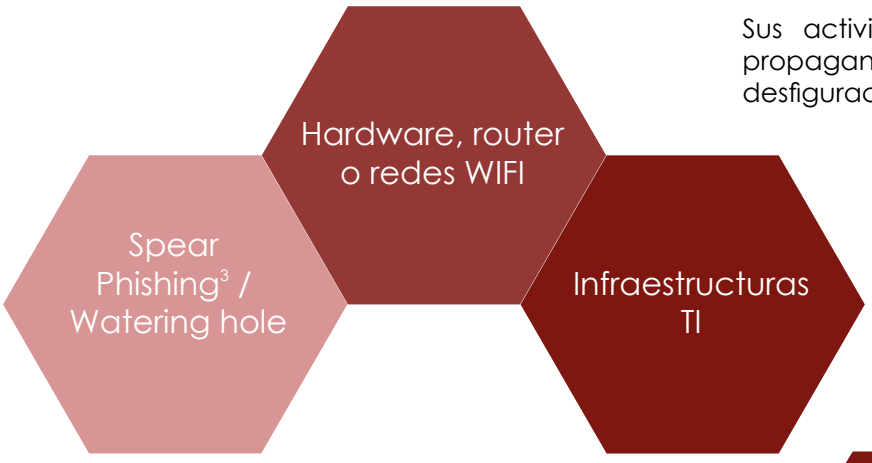
Con mayor frecuencia que en años precedentes, los ciberdelincuentes han dirigido sus **ataques contra los sistemas de empresas, bancos y otras instituciones financieras** (los llamados objetivos de alto valor), en lugar de dirigirse solo a los consumidores.

Además, en 2017, se confirmó la tendencia a **dirigir los ataques a organizaciones concretas** (como escuelas, hospitales u otras instituciones sanitarias) en las que el impacto es mayor que en ataques no dirigidos, es decir, sin víctimas concretas.

CIBERTERRORISMO Y CIBERYIHADISMO

Los grupos yihadistas y terroristas constituyen la principal amenaza, aunque todavía no parecen ser capaces de desarrollar ciberataques sofisticados.

Sus actividades más evidentes, de naturaleza propagandística, han sido ataques DDoS y desfiguraciones[4].



Métodos de ataque

3. Spear phishing: phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo.
4. Deface o Defacement (desfigurar o desfiguración): deformación o cambio producido de manera intencionada en una página web legítima a través de algún tipo de acceso de código dañino.

HACKTIVISTAS[5] EN EL CIBERESPACIO

La amenaza que suponen los grupos hacktivistas, que por regla general llevan a cabo **ciberataques por razones ideológicas**, podría crecer a la vista de la mayor disponibilidad de productos, servicios y herramientas para desarrollar ataques con un significativo impacto social.

CIBERVÁNDALOS Y *SCRIPT KIDDIES*

La **disponibilidad pública de herramientas para la comisión de ataques** tiene especial incidencia en las acciones de estos grupos, que actúan para demostrar sus propias capacidades.

ACTORES INTERNOS

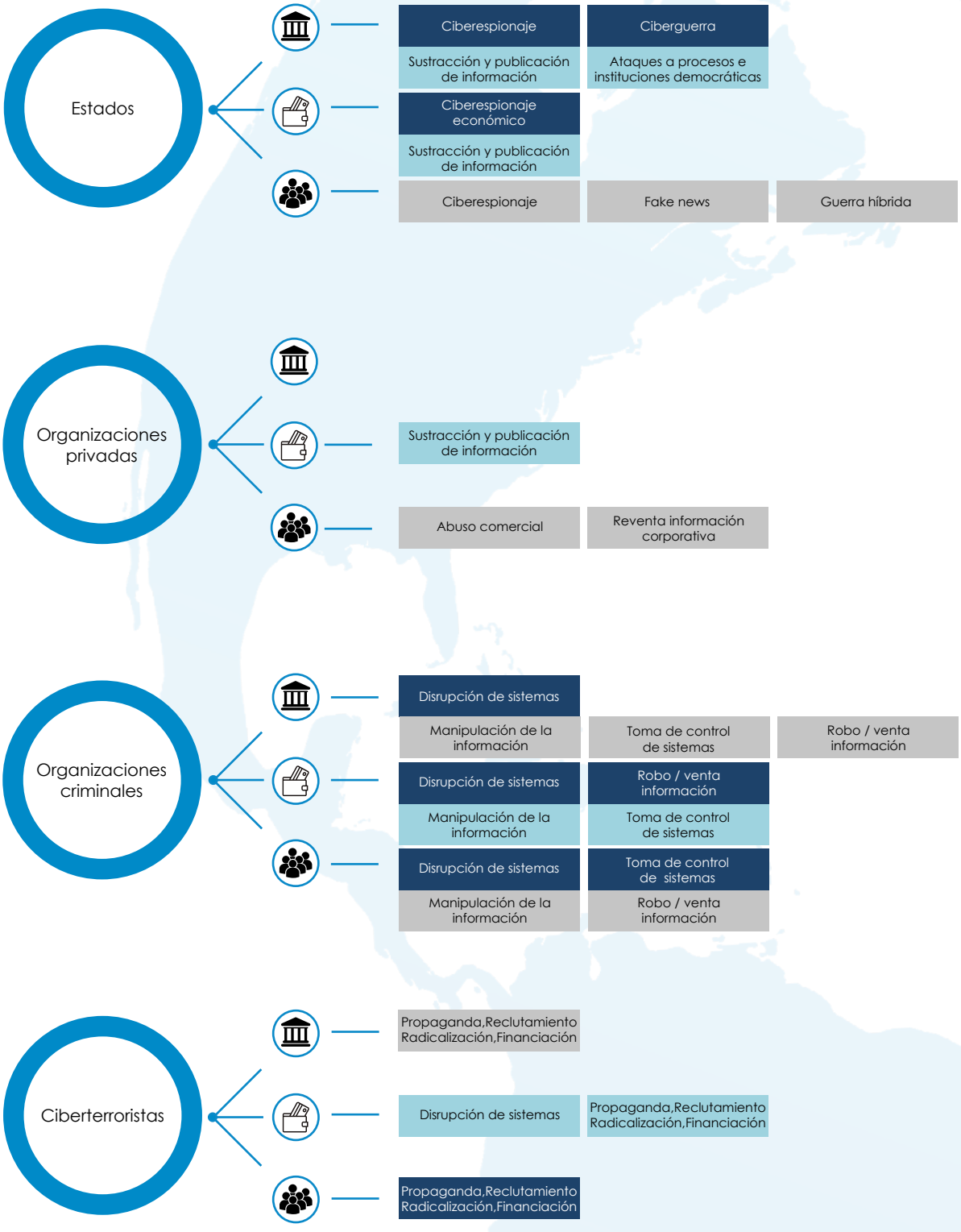
Estas acciones **no han cambiado sustancialmente en 2017.** La motivación de los ataques perpetrados ha sido de naturaleza personal o resultado de comportamientos inconscientes o descuidados.

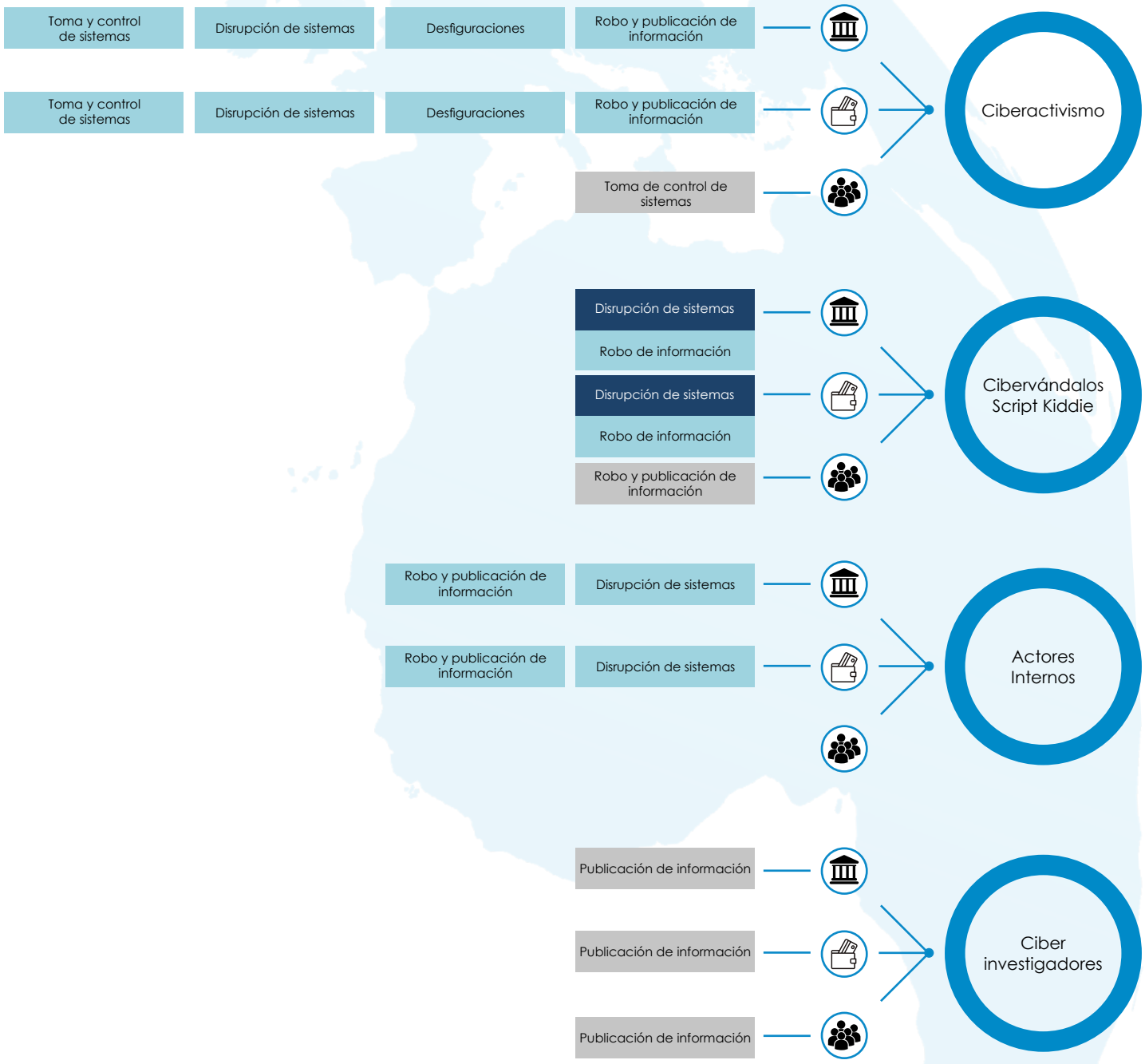
ORGANIZACIONES PRIVADAS

Como se muestra en el siguiente gráfico, las características y, correlativamente, los motivos de los ciberataques desarrollados por organizaciones privadas pueden ser de distintos tipos.

5. Hacktivismo o ciberactivismo. Activismo digital antisocial. Sus practicantes persiguen el control de ordenadores o sitios web para promover su causa, defender su posicionamiento político, o interrumpir servicios, impidiendo o dificultando el uso legítimo de los mismos

CIBERAMENAZAS 2017





Leyenda

Agentes de la amenaza

Víctima

- Sector público
- Organización privada
- Ciudadanos

Nivel de peligrosidad de la amenaza

- No han aparecido nuevas amenazas
  Existen suficientes medidas para eliminar la amenaza
  No han existido incidentes apreciables derivados de la amenaza
- Nuevas tendencias asociadas a la amenaza
  Medidas limitadas para eliminar la amenaza
  El número de incidentes no ha sido especialmente significativo
- Desarrollos relacionados con la amenaza
  Las medidas tienen efecto limitado en la amenaza
  Significativo número de incidentes derivados de la amenaza

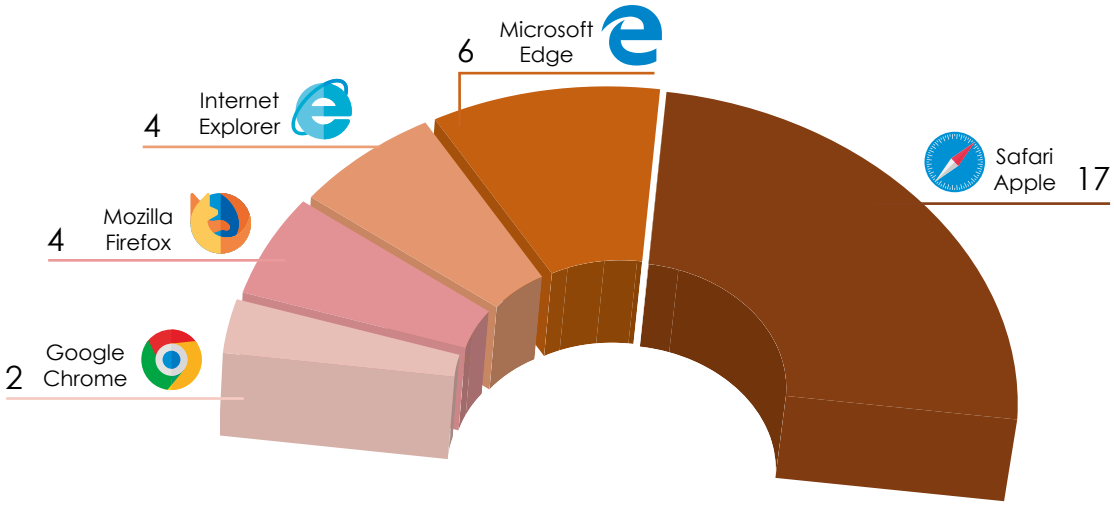
Fuente: Cyber Security Assessment Netherlands. CSAN 2017 y elaboración propia.

4 VULNERABILIDADES

En este epígrafe se detallan las vulnerabilidades más significativas de 2017.

NAVEGADORES E INFRAESTRUCTURAS WEB

En un reciente informe del Google *Proyect Zero*, se muestra que todos los navegadores de escritorio conocidos tienen **vulnerabilidades de seguridad** asociadas.



Además, la importante **adopción de CMS[6] por parte de sitios** web los convierte en objetivos especialmente tentadores para los atacantes, debido a que presentan vulnerabilidades resultado de la **utilización de** *plugins*[7] o extensiones desactualizadas, tales como WP *Statistics* (plugin de WordPress[8]).

HARDWARE Y FIRMWARE[9]

Aunque **no es conocido el código dañino capaz de explotar estas vulnerabilidades**, su profundidad en la arquitectura del hardware hace que sea muy difícil de detectar. Ejemplo de ello es **Spectre**, una vulnerabilidad del hardware que permitiría al atacante obtener información almacenada en programas o procesos.

Aunque los fabricantes implicados ya han anunciado su respuesta a estas vulnerabilidades, **la eficacia de las actualizaciones de seguridad no podrá evidenciarse de forma inmediata.**

6. CMS: Sistema de Gestión de Contenidos
7. Plugin: aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica.
8. Wordpress: sistema de gestión de contenidos o CMS enfocado a la creación de cualquier tipo de página web.
9. Firmware: funciona como el nexo de unión entre las instrucciones (software), que llegan al dispositivo desde el exterior, y las diversas partes electrónicas (hardware).

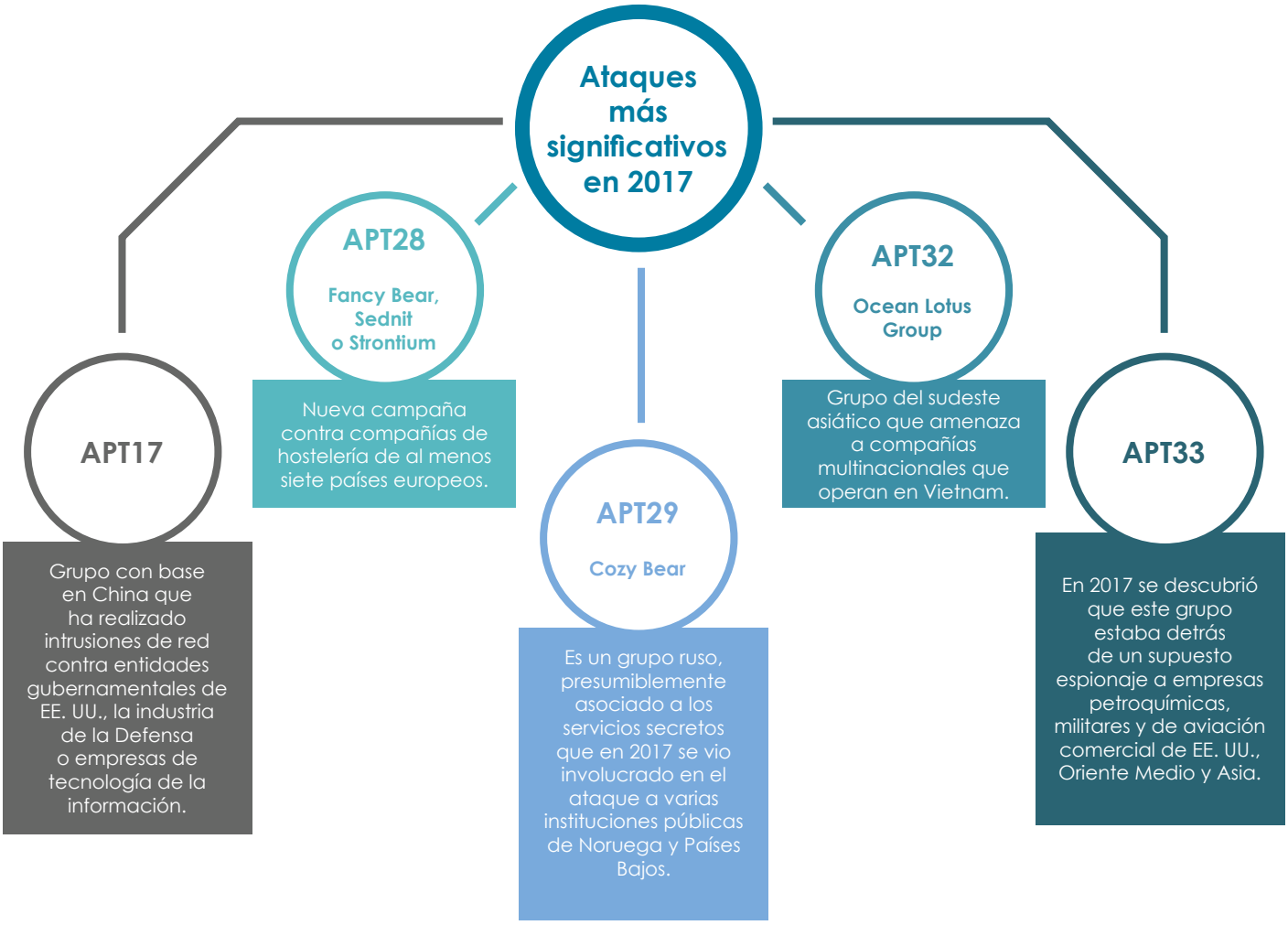
LA CIBERAMENAZA EN 2017

5

Técnicas como el ransomware[10] o las APTs[11] siguen siendo las preferidas por los grupos delincuenciales y los estados, respectivamente. En todo caso, siempre a la búsqueda de nuevas formas más eficaces. Sobre dichos avances versa este epígrafe.

APT (AMENAZA PERSISTENTE AVANZADA)

Este **ataque selectivo de ciberespionaje,** dirigido por un Estado, emplea diversos tipos de malware para proceder al robo de propiedad intelectual, tratando de permanecer oculto el mayor tiempo posible.



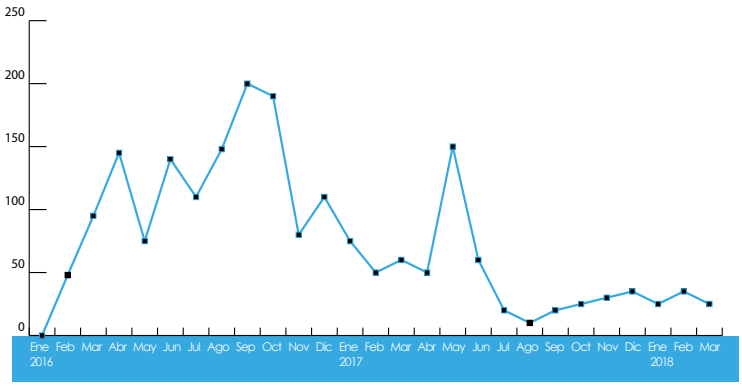
10. Ransomware: código malicioso para secuestrar datos. Forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado.
11. APT (Advanced Persistent Threat /Amenaza persistente avanzada): se trata de un ataque selectivo de ciberespionaje o cibersabotaje llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política.

ATAQUES CONTRA LA INDUSTRIA DE LA PUBLICIDAD

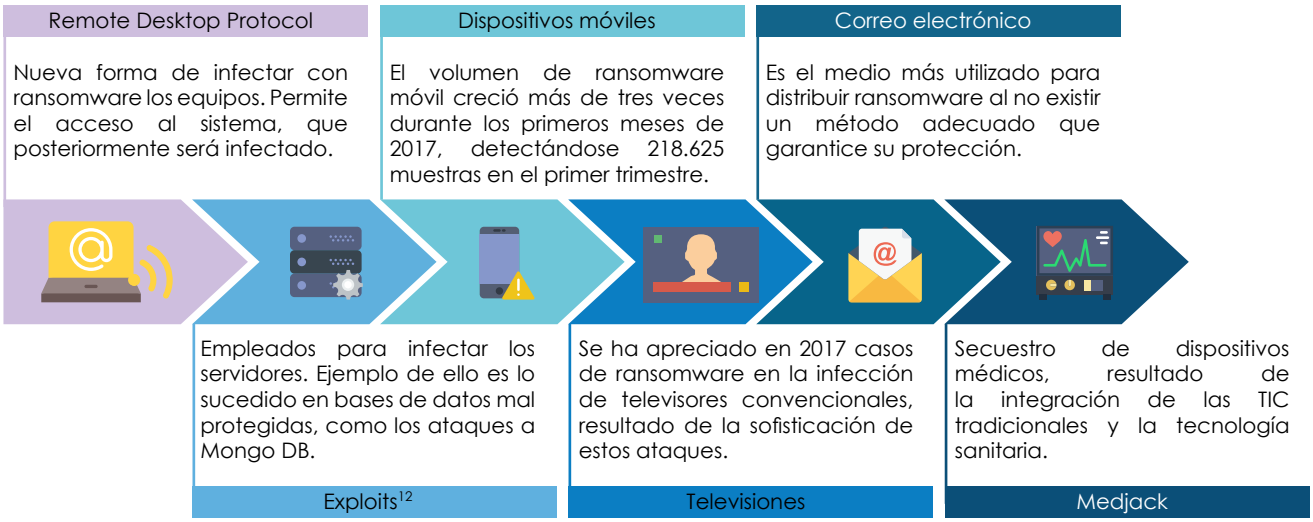
Infectar sistemas mediante la **distribución de código dañino a través de anuncios** en sitios web (lo que se denomina "*publicidad dañina*" o "*malvertising*") parece seguir en aumento. La empresa RiskIQ informó de un **incremento del 132% en el número total de casos de publicidad maliciosa** en todo el mundo. Según las cifras de PageFair, para combatir estos ataques se ha aumentado en torno a un 20% el uso de adblockers.

RANSOMWARE

A pesar de que el ransomware ha proseguido su sofisticación en los últimos años, se ha apreciado un **descenso en el número de ataques.**



En el siguiente diagrama se muestran algunas de **las modalidades de infección mediante ransomware** empleadas en 2017.



Durante 2017 se han detectado evidencias de que **el sector sanitario es el más frecuentemente atacado por esta amenaza.**

12. Exploit: Programa que explota o aprovecha una vulnerabilidad de un sistema informático en beneficio propio. Exploit día cero: aprovechamiento de una vulnerabilidad inmediatamente después de haber sido descubierta. Se beneficia del lapso de tiempo requerido por los fabricantes para reparar las vulnerabilidades reportadas.

PHISHING Y SPAMMING

En 2017, **las campañas de phishing[13] aumentaron tanto en volumen como en sofisticación.** Este método constituye el vector de infección más exitoso, tanto en ataques dirigidos (ciberespionaje) como innominados (ransomware). En la actualidad, los ataques buscan objetivos concretos, convirtiéndose así en ataques más específicos.

Spear phishing	Método adaptado al objetivo que se emplea para atacar a una entidad concreta. Es difícil determinar su naturaleza dañina puesto que generalmente utiliza una recopilación de todo tipo de información pública.
Nuevo método de ataque que se contrata a cibercriminales y que permite obtener contraseñas de las víctimas simulando páginas web de servicio al usuario como Gmail, Facebook o Yahoo.	**Phishing as a service**
BEC / Whalling[14]	Ataques de spear-phishing contra ejecutivos de alto nivel, generalmente con el objetivo de sustraer dinero de sus organizaciones o de sus víctimas. También puede ser empleado para realizar ciberespionaje.

El spam[15], por su parte, ha ganado en calidad, aunque el número de ataques a través de este tipo de mensajes parece haber descendido. No obstante, sigue siendo el principal medio para la **entrega innominada de código dañino** a través de archivos adjuntos y URL[16] dañinas.

INTERNET OF THINGS (IOT) - BOTNETS

Las vulnerabilidades de los dispositivos Internet of Things (IoT, dispositivos cotidianos conectados a Internet), tales como la **ausencia de cifrado** a las escasas e inexistentes **actualizaciones de software** han sido especialmente explotadas en 2017 para espiar a sus usuarios o para manipular su entorno.

En este periodo de tiempo, se han empleado numerosos dispositivos como routers, cámaras web o receptores de televisión digital para llevar a cabo **ataques DDoS** o de **ransomware basados en botnets[17].**

La posibilidad de perpetrar este tipo de acciones se sustenta, en muchas ocasiones, en la disponibilidad pública de las herramientas de ataque.

13. Phishing: método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.
14. Whalling: "pesca de ballenas o peces gordos", en referencia a los más altos cargos ejecutivos de la organización.
15. Spam: correo electrónico no deseado que se envía aleatoriamente en procesos por lotes.
16. URL (Uniform Resource Locator / Localizador Uniforme de Recursos): Los documentos de texto, las fotografías y los audios, entre otros tipos de contenidos digitales, tienen un URL cuando se publican en Internet y sirve para que puedan ser localizados.
17. Botnet: Red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando desee lanzar un ataque masivo, tal como envío de correo basura o denegación [distribuida] de servicio

ATAQUES DE DENEGACIÓN DE SERVICIOS (DDoS)

Según el estudio realizado por Kaspersky, **un 33% de las organizaciones se enfrentaron en 2017 a un ataque DDoS,** un 16% de empresas más que en 2016. Estos datos evidencian que estos ataques, además de haber aumentado con respecto al año anterior, también han incrementado su tamaño (*a finales de 2017, la botnet Mirai fue protagonista del mayor ataque DDoS de la historia por ancho de banda, más de 1 Tbps*).

TIPOLOGÍA DE LOS ATAQUES

DISPOSITIVOS IOT

El número de dispositivos IoT vulnerables ha contribuido al aumento del tamaño de los ataques DDoS.

DDoS AS A SERVICE

En desarrollo debido a la reducción del coste de las herramientas precisas para perpetrarlos.

DDoS BASADOS EN DNS

En aumento en 2017, tras las acciones contra el servicio DNS[18] del la empresa DYN.

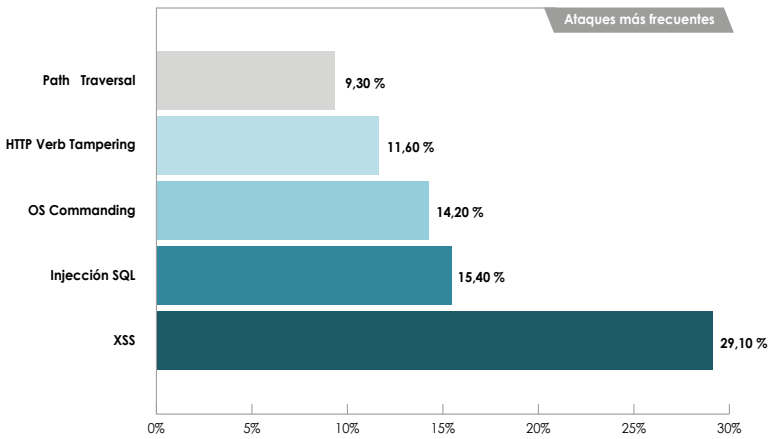
EXTORSIÓN

Acciones de extorsión bajo amenaza de ataques DDoS o de interrupción de servicios en línea.

ATAQUES WEB

El 40% de los ataques web están dirigidos a la **obtención de información,** siendo las aplicaciones web patrocinadas por el sector público y el financiero las que mayor número de ataques han reportado en 2017. Los vectores de agresión más significativos durante el 2017 fueron, según la empresa Positive Technologies, el Cross Site Scripting (XSS) y la inyección SQL.

Asimismo, los ataques basados en web, que hacen uso de sus sistemas y servicios habilitados, han sido en 2017 una de las amenazas más importantes y que perdurará en los próximos años.



Datos del 4º trimestre de 2017
Fuente: Positive Technologies

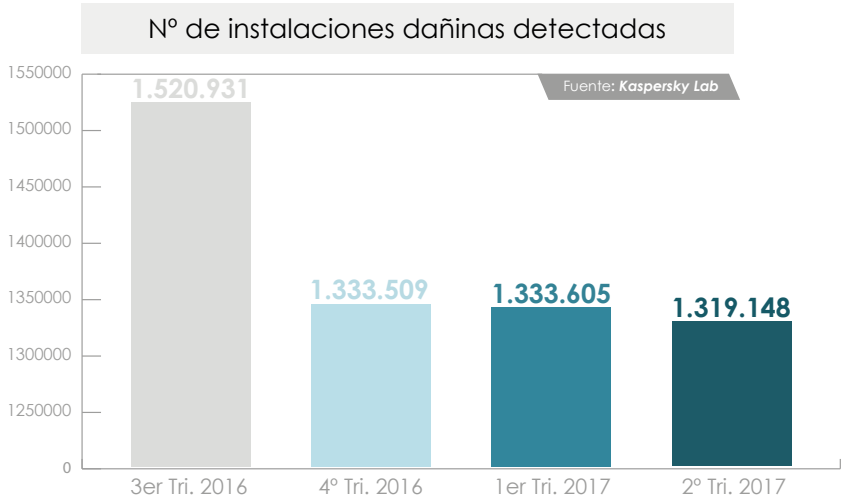
18. DNS (Domain Name System / Sistema de nombre de dominio): es un sistema que nombra a todos los equipos, servicios o recursos conectados otorgándoles una dirección.

Código dañino

En 2017, el código dañino siguió evolucionando en términos de sofisticación y diversidad, aunque puede apreciarse una ligera disminución en términos de frecuencia.

Dispositivos móviles

A pesar de haber descendido en número absoluto, el código dañino para dispositivos móviles ha mejorado su nivel de sofisticación.



Sector financiero

En los ataques a estas entidades se emplearon desde correos de ***spear phishing*** o **código dañino para cajeros automáticos** hasta ataques de ***watering hole*** *(los ataques de este tipo intentaron infectar en 2017 a más de 100 organizaciones, en 31 países diferentes)*.

Exploit-kits

Aunque en 2017 el número de exploit-kits[19] se redujo significativamente, algunas de las campañas de código dañino más significativas utilizaron este tipo de ataque para comprometer a sus objetivos.

Las filtraciones de herramientas y exploits han configurado también la realidad de 2017. La filtración de determinado código dañino *(cuyo desarrollo originario se atribuyó a actores estatales)* dio lugar a los **ataques *WannaCry* y *NotPetya*.**

19. Exploit- kits: conjunto de herramientas automáticas de ataque que aprovechan una o varias vulnerabilidades.

6 MEDIDAS DE PROTECCIÓN

En este epígrafe se desarrollan los ciberincidentes más significativos de 2017, agrupados por las motivaciones de los agentes de las amenazas.

MEDIDAS DIRIGIDAS A LOS INDIVIDUOS

Los navegadores de Internet están implementando medidas para mantener a los usuarios mejor informados. Por ejemplo, Google Chrome y Mozilla Firefox han anunciado el señalamiento como inseguros de **todos los sitios web que no usen protocolo HTTPS;** medida que podría alentar a los propietarios de sitios web a implantar dicho protocolo por su mayor seguridad.

En este sentido, el **CCN-CERT ha llevado a cabo una campaña de impulso a la implementación del protocolo HTTPS** en las sedes electrónicas del sector público, poniendo a disposición de dichos organismos un informe personalizado del análisis HTTPS y un documento de recomendaciones para su correcta implantación.

Asimismo, otra medida para proteger a los individuos de posibles engaños es a través de los **certificados *domain validate*** *(certificado que acredita que un usuario es titular de un dominio)*.

MEDIDAS DIRIGIDAS A LAS ORGANIZACIONES

Seguridad en los proveedores

A pesar de que las grandes organizaciones son, en general, capaces de organizar y gestionar adecuadamente su seguridad a través de políticas, procedimientos y medidas específicas; con frecuencia hacen uso de proveedores en los que el nivel de madurez es más bajo.

En los Países Bajos, en febrero de 2017 se prohibió la transferencia digital de los resultados electorales, ante la posible vulnerabilidad del software de apoyo para el recuento final de las mesas electorales.

Ataques por Ransomware y DDoS

Las grandes organizaciones suelen salir airosas de los ataques por ransomware o DDoS invirtiendo en procesos y herramientas de mitigación. Sin embargo, la protección contra ataques a gran escala -como los acaecidos con la botnet Mirai- es siempre difícil.

Cuando tales acciones afectan a organizaciones más pequeñas, suele carecerse de la experiencia debida y de los medios económicos para invertir en la mitigación de ataques DDoS o de infecciones por ransomware.

MEDIDAS DIRIGIDAS A LA TECNOLOGÍA

MENSAJES SMS

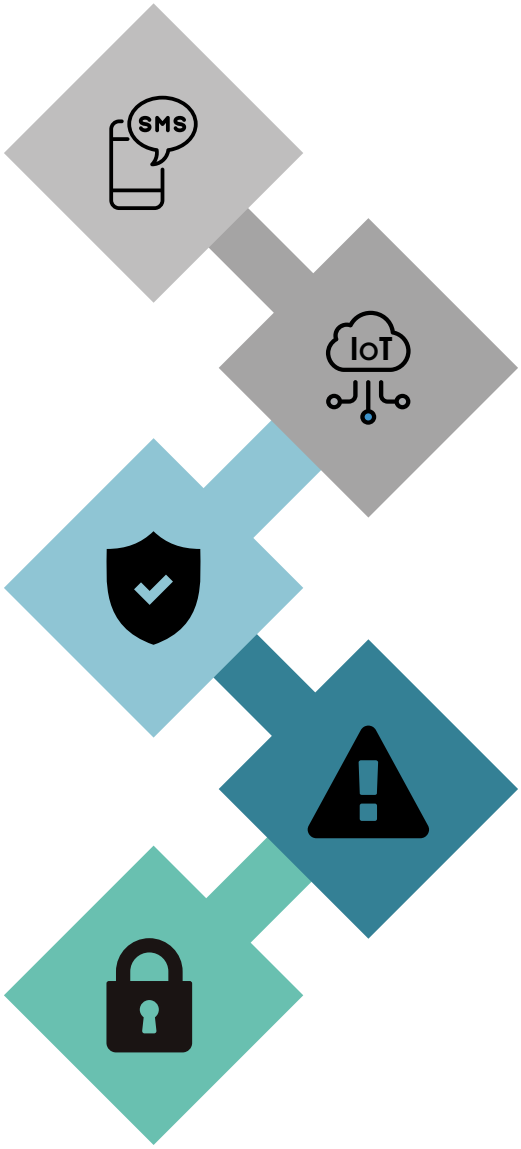
Los dispositivos Android e iOS son susceptibles de sufrir ciberataques que permiten acceder a los mensajes SMS recibidos a través del ordenador del destinatario. Por tanto, el empleo de SMS representa una amenaza para la autenticación de dos factores.

SEGURIDAD DE LOS PRODUCTOS

El CCN publicó en 2017 un Catálogo de Productos de Seguridad TIC que recoge en un listado aquellos productos que cuentan con las certificaciones indicadas para ser empleados en sistemas que demanden altos niveles de seguridad.

LA NECESIDAD DEL CIFRADO

Estados europeos, como los Países Bajos, han hecho obligatorio el uso de HTTPS en los sitios web gubernamentales. Además, esta necesidad se ha extendido a las aplicaciones de mensajería instantánea, como Telegram o WhatsApp, que ya emplean el cifrado de extremo a extremo.



THE INTERNET OF THINGS

Todavía no hay una solución clara para los efectos secundarios no deseados de Internet of Things. La falta de sostenibilidad TIC seguirá siendo un problema si el sector no puede regularse a sí mismo.

VULNERABILIDADES ESENCIALES

En 2017 se han publicado diferentes estudios referidos a la explotación de vulnerabilidades ligadas al software, como *Dedup Est Machina*, que explota la duplicación de memoria para tomar el control de un navegador.

Marco estratégico y legal

En **España**, en 2018, se han publicado dos nuevas **Instrucciones Técnicas de Seguridad:**

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de **Auditoría de la Seguridad** de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de **Notificación de Incidentes de Seguridad.**

Ambas, se suman a las ITS de **Conformidad con el Esquema Nacional de Seguridad (ENS)** y del **Informe de Estado de Seguridad** publicadas con anterioridad.

Por otro lado, está culminando el proceso de transposición de la Directiva (UE) 2016/1148, de 6 de julio, Directiva NIS, que afectará también al Sector Público, y que, entre otras cuestiones:

- Identificará los Operadores de Servicios Esenciales.
- Las medidas de Seguridad que habrán de aplicar.
- Las Autoridades competentes.
- Identificará los CSIRTs de referencia.
- Asignará al CCN-CERT la coordinación y respuesta técnica en casos de especial gravedad.

Además de ello, y como consecuencia de la plena aplicación del Reglamento (UE) 2016/679 de 27 de abril de tratamiento y libre circulación de datos personales (Reglamento General de Protección de Datos), se ha elaborado un **Proyecto de nueva Ley Orgánica de Protección de Datos** que, derogando la ley vigente, entrará a regular aquellas cuestiones que el Reglamento General de Protección de Datos deja a la consideración de los estados miembros.

Actividad europea

- **Propuesta de la Comisión Europea para reemplazar la directiva e-Privacy** por una regulación cuyo alcance cubra otros servicios de comunicaciones en capas superiores del sistema, además de los tradicionales proveedores de telecomunicaciones.

- Establecimiento de la **Estrategia de Ciberseguridad de la UE.**

- **Adopción de la Directiva NIS** sobre seguridad de las redes y los sistemas de información.

- **Propuesta de Reglamento del Parlamento Europeo y del Consejo** relativo a la certificación de la ciberseguridad de las TIC.

- Anuncio de la Comisión para la **evaluación y revisión del Reglamento (UE) n.º 526/2013** del Parlamento Europeo y del Consejo, que podría conducir a una posible reforma de la Agencia y a un reforzamiento de sus facultades y capacidades para apoyar a los Estados miembros de manera sostenible.

ACTIVIDAD CCN-CERT DEL CENTRO CRIPTOLÓGICO NACIONAL

DESARROLLO DE SOLUCIONES

ATENEA es la nueva **herramienta formativa de desafíos de ciberseguridad** que pretende concienciar sobre la importancia de este campo.

Gloria es la plataforma para la **gestión de incidentes y amenazas** de ciberseguridad, que además se ha integrado con las herramientas Carmen, Lucía y Reyes para favorecer la detección, el análisis y el intercambio de incidentes.

El **Servicio de Alerta Temprana para Sistemas de Control Industrial** tiene como función principal la **detección temprana de incidentes** de seguridad. Permite, además, el acceso a un mayor número de reglas de detección y la correlación de eventos, favoreciendo el soporte a la resolución de incidentes

FORMACIÓN

El Centro Criptológico Nacional ha elaborado en 2017 más de 146 guías e informes y ha impartido, además, cursos de formación, tanto presenciales como a distancia.

RESPUESTA A CIBERATAQUES

Saguaro
Actor mexicano enfocado en el robo de credenciales. Más de 60.000 IPs diferentes afectadas y más de 36 países afectados.

STRUTS
Vulnerabilidad que afectó a millones de servidores web conectados a Internet. En España, 75 organismos afectados, seis de ellos con impacto crítico.

NotPetya
Ataque a la cadena de suministros en Ucrania con robo de credenciales. Empleo del exploit Eternalblue para su propagación.

Enero 2017 | *Febrero 2017* | *Marzo 2017* | *Mayo 2017* | *Junio 2017* | *Octubre 2017*

Owncloud
Suite que permitía tener un servidor en una nube privada. Explotación de varias vulnerabilidades, acceso a archivos y ejecución de código.
Diez entidades afectadas. Algunas de ellas siguen siendo vulnerables.

Wannacry
El CCN desarrolló la vacuna NoMoreCryv0.1. y además publicó un informe de código dañino, Ransom. WannaCry. A día de hoy, se sigue actualizando la herramienta.

#OpCatalunya
Campaña de cuatro fases contra AAPP y empresas. Ataques de DDoS a más de 70 páginas. Además, se emplearon las redes sociales para aumentar la visibilidad y coordinación.

7 TENDENCIAS

Es de esperar que los futuros ciberataques incrementen su grado de sofisticación, de virulencia y de osadía. Los siguientes son algunos ejemplos que desarrollan las tendencias de un inmediato futuro.

EXPLOITS-KITS

La disminución del número de vulnerabilidades atacables provocará un descenso en el uso de exploits-kits (aunque seguirán siendo utilizados en aquellas regiones geográficas donde no puedan ser monitoreados por los investigadores). Por ello, se dará paso a "kits humanos" donde los agentes de las amenazas cambiarán su modelo comercial para lograr sus objetivos atacando las **debilidades humanas**.

ATAQUES POR DENEGACIÓN DE SERVICIOS

Todo apunta al aumento de este tipo de ataques, con algunas variantes:

- **Denegación de Servicio Permanente (PDoS)** para las operaciones de Centros de Datos y dispositivos IoT.
- Mayor importancia y sofisticación de los ataques DoS de telefonía (TDoS).
- Aumento de segmentación (e incluso personales) de los **ataques de denegación de servicio combinados con ciber-rescate (Ransom-DoS).**
- Los sistemas sanitarios podrían convertirse en un nuevo objetivo.

CIBERESPIONAJE

Los expertos esperan un **crecimiento del ciberespionaje** debido a desencadenantes geopolíticos, sanciones económicas u objetivos estratégicos de las naciones. Para ello, a pesar de que **continuarán empleando APTs**, se están creando nuevas técnicas y herramientas que permitan robar la propiedad intelectual y los secretos de sus objetivos.

RANSOMWARE

En el futuro inmediato se va a producir un **incremento de ataques dirigidos contra objetivos concretos.** Por ejemplo, contra dispositivos sanitarios.

INCREMENTO DE LAS BRECHAS DE SEGURIDAD

Analistas, como Tyler Moffitt de Webroot, coinciden en señalar que en los próximos meses se producirán significativas brechas de seguridad que **podrán afectar, al menos, a 100 millones de cuentas;** amenaza que, según la empresa Imperva, se extenderá a la filtración masiva de datos en la nube.

ADOPCIÓN DE LA BIOMETRÍA

La empresa Webroot ha señalado que en los próximos meses se verán los primeros exploits dirigidos al acceso biométrico, sustentado en reconocimiento facial o huellas dactilares.

INTELIGENCIA ARTIFICIAL Y APRENDIZAJE AUTOMÁTICO

La industria de la seguridad comenzará a utilizar más automatización, aprendizaje automático e inteligencia artificial para combatir los ciberataques, tal y como ha señalado la empresa FireEye.

AMENAZAS MÓVILES

En los próximos meses, según la empresa Webroot, se verá la primera gran infección de malware en la App Store de Android. Otras empresas sostienen, por su parte, que 2018 y 2019 serán testigo del primer ransomware móvil diseminado, probablemente, a través de SMS/MMS.

Regulación Internet of Things

Podría ser el sector más afectado por las brechas Meltdown y Spectre, aun cuando muchos especialistas coinciden en que la legislación será el mayor cambio. No es de extrañar que sucesos como los ocurridos con la *botnet Mirai* se repitan pero, esta vez, con poca capacidad de respuesta.

Delincuencia más sofisticada

En los próximos años, los ciberdelincuentes aprovecharán los kits de hacking a partir de herramientas filtradas o sustraídas de agencias de inteligencia patrocinadas por Estados.

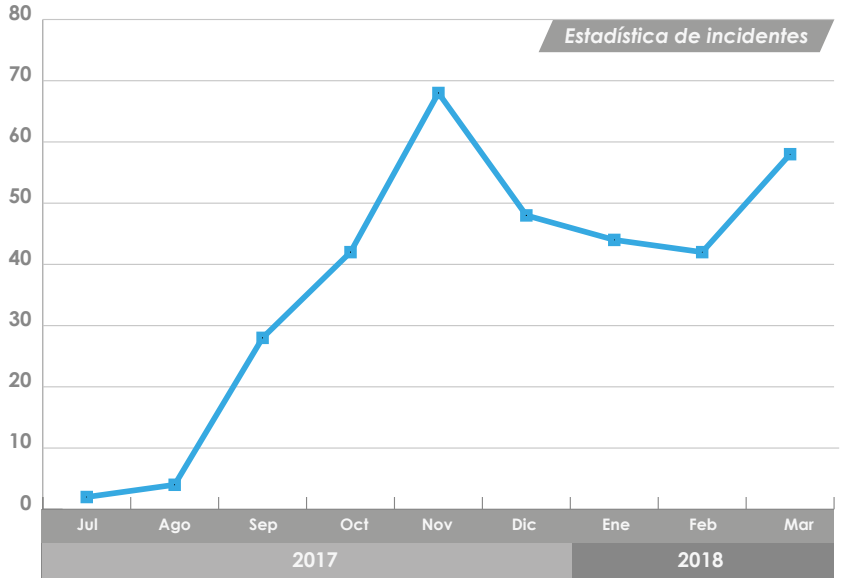
Ataques contra redes sociales

Es presumible que los próximos meses se desarrollen formas más asequibles para los atacantes gracias a las redes sociales, que pueden ser empleadas para sofisticadas actividades de ingeniería social y reconocimiento.

Como señala Airbus Cybersecurity, para protegerse de estos ataques, las organizaciones deben implementar políticas de seguridad, como programas de formación para los empleados, y la creación de planes de respuesta a incidentes que coordinen las actividades de los departamentos legal, de recursos humanos, marketing y TI.

CRIPTOMINING

Se prevé que este proceso de generación de criptomonedas continúe creciendo a lo largo de 2018, debido a que cada vez más **familias de malware** incluyen funcionalidades de minería en su arsenal de ataque. Asimismo, la tendencia actual apunta también al **empleo de los navegadores** para el minado de monedas, siendo **JavaScript** la tecnología más usada.

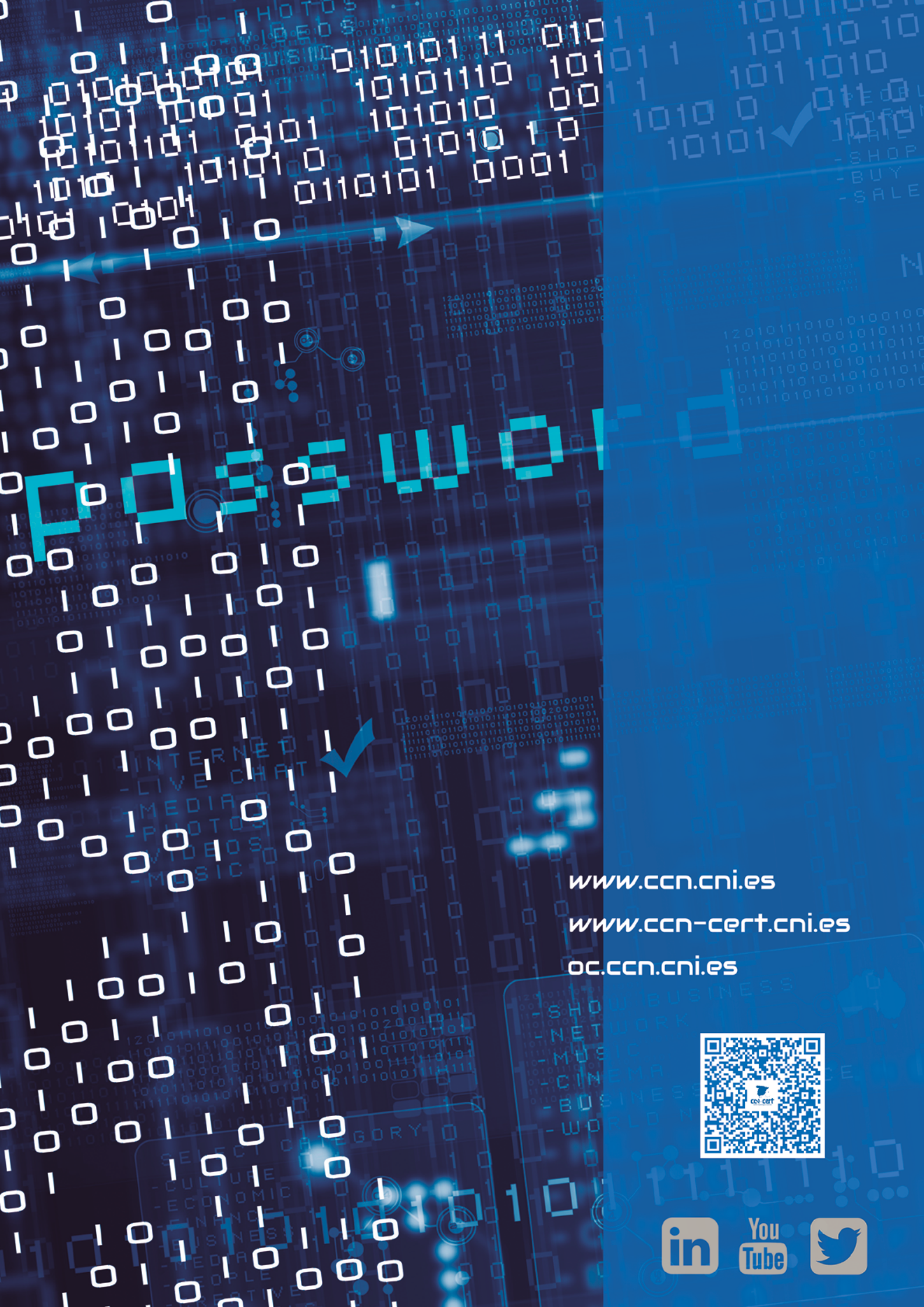


CÓDIGO DAÑINO SIN ARCHIVOS

Digital Pathways ha aseverado que los "ataques sin archivos" se tomarán más en serio y **serán una amenaza de igual potencia que los troyanos;** pues "este tipo de código dañino reside en la memoria del PC y permanece allí hasta que se reinicie. Un antivirus normal no detectará estos ataques".

MAYOR USO DE MSSP

Buena parte de las medidas de seguridad vendrán dadas por los **Proveedores de Servicios Gestionados de Seguridad (MSSP),** que serán objeto de un mayor interés por parte de las organizaciones que reconocen que el nivel de esfuerzo y la experiencia interna requerida para un Centro de Operaciones de Ciberseguridad con garantías de éxito se encuentran más allá de sus posibilidades. Así lo ha asegurado la entidad Resolve.



www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es