Eleven Paths

#CyberSecurityReport 18H2

innovationlab@11paths.com
elevenpaths.com

Telefónica CYBER SECURITY UNIT

Durante el 2018 se han publicado numerosas noticias relacionadas con la ciberseguridad. Desde la entrada en vigor de la RGPD, hasta el escándalo de Cambridge Analytica, **la privacidad en la red es ya una prioridad para los usuarios y los gobiernos.** De ese modo, las noticias sobre brechas de seguridad que dejan al descubierto datos de usuarios ocupan ahora los diarios y páginas de información generalistas. Además, los ataques perpetrados por grupos profesionales ya no son asuntos privados. Las supuestas injerencias en elecciones, historias de espionajes y ataques sofisticados también son de dominio público, tanto para profesionales del sector como para el público en general.

La ciberseguridad está tan presente que se mezcla ya de forma natural con la información general, algo impensable hace solo algunos años. De hecho, el **World Economic Forum situó los ciberataques entre los tres primeros riesgos globales en 2018,** y se estima que el **cibercrimen tiene un coste que ya roza el medio billón (millón de millones) de euros anual.**

No obstante, esto no significa que se entienda, se analice correctamente y por tanto se aproveche esta avalancha de información para mejorar los procesos y ser menos vulnerables. La falta de información es tan perjudicial como su exceso. **No solo se debe estar al día e informar, sino que es necesario analizar y saber priorizar, conocer qué es importante y por qué.**

Tanto si es aficionado como profesional, es importante que sea capaz de seguir el ritmo de las noticias relevantes sobre ciberseguridad: ¿qué es lo más relevante que está pasando? ¿Cuál es el panorama actual? ¿Cómo evolucionan los problemas de seguridad, vulnerabilidades y ataques? **Se hace necesario sintetizar, sin perder profundidad.**

Por todo ello, el objetivo de este informe es sintetizar la información sobre ciberseguridad de los últimos meses **(desde la seguridad en móviles hasta el ciberriesgo, desde las noticias más relevantes hasta las más técnicas y las vulnerabilidades más habituales)**, tomando un punto de vista que abarque la mayoría de los aspectos de esta disciplina, para así ayudar al lector a **comprender los riesgos del panorama actual.**

El lector dispondrá así de una herramienta para comprender el estado de la seguridad desde diferentes perspectivas, y podrá conocer su estado actual y proyectar posibles tendencias a corto plazo.

La información recogida se basa en buena parte en la recopilación y síntesis de datos internos, contrastados con información pública de fuentes que consideramos de calidad.

CONTENIDOS

LOS INCIDENTES MÁS DESTACADOS DEL SEGUNDO SEMESTRE DE 2018

Durante el segundo semestre de 2018 la ciberseguridad ha vuelto a copar titulares generalistas, señal inequívoca de la importancia e influencia que ejerce ya en todos los ámbitos de la sociedad, desde los aspectos políticos a los económicos, pasando por componentes sociales. Destacamos los hechos más relevantes ocurridos durante este período.

julio

Magecart

Magecart el skimmer virtual y nombre del grupo cibercriminal creador de sus creadores, **ataca a más de 800 sitios de comercio electrónico previamente comprometidos**. Magecart inyecta sencillos JavaScripts en el navegador para robar los datos de tarjetas de crédito e identidad de los usuarios mientras los utilizan en la web legítima. Culminaría su mayor hazaña contra la página de British Airways semanas más tarde.

VPNFilter

Malware avanzado dirigido a dispositivos IoT y atribuido al grupo APT28, podría estar **detrás de los ataques a los sistemas SCADA de una central ucraniana** de destilación de cloro.

Interferencia en elecciones al congreso de EE. UU.

Microsoft afirma que grupos de inteligencia **rusos podrían haber interferido en las elecciones al congreso de los Estados Unidos** de ese mismo año.

agosto

Coinhive

Más de **200.000 routers del fabricante MikroTik afectados por un 0-day fueron comprometidos** y manipulados para inyectar el minero Coinhive en el tráfico web de los usuarios.

Malware en Taiwan

Un malware afecta a varias compañías taiwanesas de fabricación de chips e **interrumpe temporalmente la producción de microprocesadores**, entre ellos, los destinados a los últimos modelos de iPhone de Apple.

Apache Struts

La vulnerabilidad de ejecución remota de código arbitrario en Apache Struts (CVE-2018-11776) **es explotada masivamente usando exploits derivados de pruebas de concepto**, para inyectar criptomineros.

septiembre

Trinity

El grupo FIN6 ataca de nuevo con el malware **"Trinity", diseñado para afectar a terminales de pago**. Los datos de millones de tarjetas de crédito son captados y transferidos para su puesta en venta en el mercado negro.

Xbash y Iron Curl

La UNIT42 de Palo Alto Network descubre el malware Xbash. Una creación del Iron Group con múltiples capacidades: ransomware, criptominado y creación de botnets. A raíz de esa investigación, **desde ElevenPaths descubrimos un repositorio con todo tipo de recursos del mismo grupo, además de una nueva creación: Iron Curl.**

Magecart

Magecart continúa haciendo estragos con nuevas campañas, una de ellas, afecta a NewEgg, un sitio de venta online con más de 50 millones de visitas al mes.

GreyEnergy
Una investigación de ESET descubre GreyEnergy, que causa **el primer apagón eléctrico causado por una ciberarma.** Bautizado como GreyEnergy, esta evolución de BlackEnergy continúa atacando objetivos principalmente localizados en Ucrania. Según ESET, sus mejoras se centran en aumentar su capacidad de permanecer oculto.

Colourama
Alojan **un paquete malicioso en los repositorios de librerías de terceros del lenguaje de programación Python, PyPi**. El paquete, denominado 'Colourama' (los autores buscaban la confusión con el paquete original 'Colorama'), poseía un mecanismo para vigilar el portapapeles y robar, en caso de ser detectado, datos de criptomoneda del usuario. Hacia finales de octubre, ya son una docena de paquetes detectados que siguen idéntico modus operandi.

Explotación de CVE-2018-15454
Cisco informa de la detección de una campaña de explotación masiva de la vulnerabilidad CVE-2018-15454, **que afecta a la implementación del protocolo SIP de sus cortafuegos.**

Explotación de CVE-2018-8589
A mediados de noviembre, la firma rusa Kaspersky informa de la **detección de exploits que aprovechan la vulnerabilidad CVE-2018-8589 (elevación de privilegios en Windows 7 y Windows Server 2008 a través de Win32k.sys**). Este exploit está relacionado con campañas APT contra entidades de oriente medio.

MoneroOcean
Investigadores de Juniper Networks, informan de la explotación de **servicios Docker mal configurados** para instalar el script de criptominería MoneroOcean.

Marriot
Marriott sufre una brecha de seguridad y **se exponen datos de 327 millones de usuarios** (pasaportes, números de seguridad social... y para algunos, incluso tarjetas de crédito) y que además habían estado expuestos al menos durante 4 años, cuando compró a Starwood ya comprometida.

Kubernetes
Se detecta un **gravísimo y primer fallo de este calibre en Kubernetes** y derivados como OpenShift. La vulnerabilidad CVE-2018-1002105 permite a un atacante elevar a administrador y así controlar cualquier nodo del cluster de contenedores. Se ven afectadas las versiones 1.0.x o 1.9.x.

API de Facebook
Se descubre un fallo en la API de Facebook **podría haber permitido a un atacante acceder a las fotografías privadas de casi 7 millones de usuarios.** Poco después se descubre que Facebook podría haber estado colaborando para ofrecer datos privados de usuarios a las grandes tecnológicas.

octubre noviembre diciembre

MÓVILES

En un mundo hiperconectado, el número de terminales no solo crece en cantidad, sino en diversidad. Móviles y tablets se han convertido en una extensión de nuestros sistemas de conexión. **Su seguridad es hoy tan relevante como la de cualquier servidor u ordenador de escritorio.**

Los sistemas operativos iOS y Android lideran la cuota de mercado. Analizamos a continuación **cómo ha evolucionado su seguridad durante los últimos meses.**

Encontrar un método para evadir la pantalla de bloqueo se ha convertido en una peculiar competición en cada nueva versión de iOS. En la versión 12 se encontraron dos fórmulas de conseguirlo, en la 12 y 12.1 aparecida precisamente para solucionar la primera.

Apple iOS

Noticias destacables

A mediados de septiembre, se publicó una prueba de concepto que producía un reinicio de los dispositivos con sistema operativo inferiores a iOS 12 (aunque afectaba a la versión beta) al visitar una página web especialmente manipulada. El problema se hallaba en el motor Webkit del navegador nativo Safari al procesar ciertas directivas.

Durante el segundo semestre se ha liberado la versión 12 del sistema operativo móvil de Apple, iOS. Al poco de ser publicado, varios usuarios reportaban que **algunos mensajes de la aplicación iMessages eran enviados erróneamente a destinatarios equivocados.**

Encontrar un método para evadir la pantalla de bloqueo se ha convertido en una peculiar competición en cada de iOS 12, el investigador José Rodríguez, descubrió **un método para evadir el bloqueo de pantalla,** obligando a la compañía a liberar un parche (12.0.1) para corregir las deficiencias.

A finales de octubre se publicó la primera revisión, la 12.1, que corrige varios errores introducidos por la nueva versión y mejora la estabilidad y optimización del sistema. De nuevo, sobre esta versión, el mismo investigador que reveló el desbloqueo de la pantalla, publica un método para **acceder a la libreta de contactos.** A comienzos de diciembre se publica iOS 12.1.1, que corrige tanto el fallo anterior como otros errores de seguridad.

Para terminar el año, el 17 de diciembre se publicó iOS 12.1.2, una actualización exclusiva para los dispositivos iPhone, dejando a los iPads en la 12.1.1. Curiosamente, además de corregir algunos fallos menores, **para los usuarios chinos la actualización iba destinada a evitar el uso de una funcionalidad que infringía una patente propiedad de Qualcomm.**

iOS 12 lo soportan, según Apple, hasta los modelos iPhone 5S en teléfonos y iPad Mini 2 (aunque iOS 10, aún con soporte, funciona en terminales iPhone 5 y el iPad de cuarta generación). Estos modelos tienen cinco y cuatro años respectivamente.

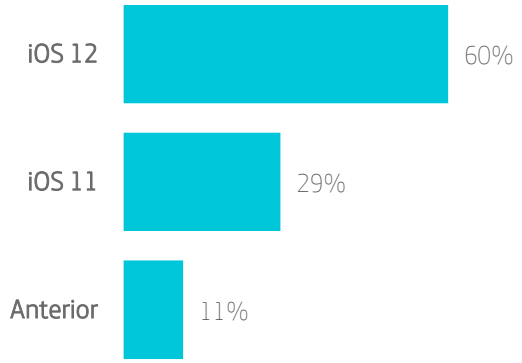
Nuevas características de seguridad[1]

Cada nueva versión del sistema operativo suele conllevar un grupo de mejoras en todas las características, incluyendo seguridad. Respecto a esto último, estas han sido las nuevas medidas implementadas en la versión 12:

- Mejora de las **funciones anti-tracking** del navegador Safari.
- Creación automática de **contraseñas robustas.**
- **Autocompletado de contraseñas** recibidas por SMS (*one-time passcodes*)
- Compartición segura de **contraseñas entre dispositivos asociados** a una misma identidad.
- Mejoras en la integración de **gestores de contraseñas** de terceros.
- Identificación de **contraseñas que hayan sido utilizadas previamente.**

Fragmentación en sistemas iOS[2]

Los datos oficiales de fragmentación de Apple iOS nos indican que un 60% de los dispositivos han adoptado iOS12, un 29% aun poseen una instalación de iOS11, mientras que el 11% cae en la categoría «Anterior» a estos.



Según datos de la App Store el 29 oct 2018.

Evolución de vulnerabilidades en iOS durante el segundo trimestre de 2018

Se han encontrado un total de **125 vulnerabilidades** de diversa gravedad, podemos ver su distribución según gravedad (de 1 a 10)

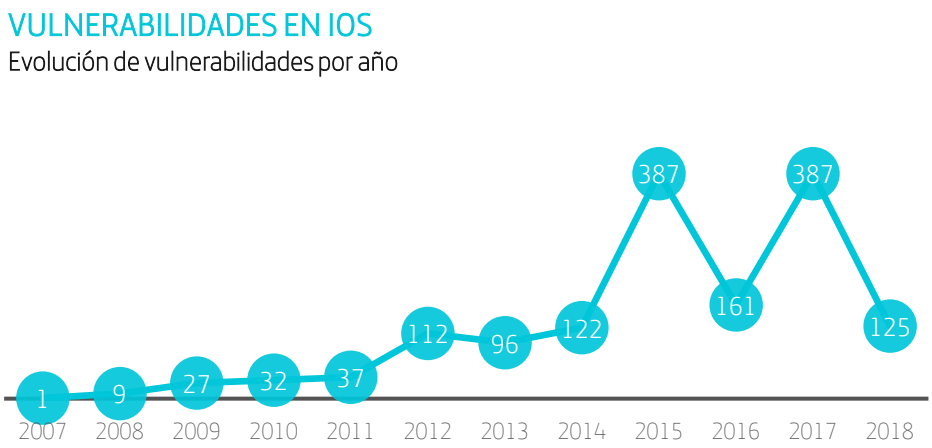
Las nuevas características de seguridad de la reciente versión de iOS están centradas en mejorar la experiencia de usuario con las contraseñas, su gestión y mejor uso.

[1] https://www.apple.com/ios/ios-12/features/

[2] https://developer.apple.com/support/app-store/

Evolución anual de vulnerabilidades en iOS

Mostramos aquí la evolución anual por número acumulado de vulnerabilidades:



El número de vulnerabilidades detectadas en iOS ha crecido sustancialmente desde 2012, con años especialmente críticos como 2015 y 2016.

Android

El 6 de agosto vio la luz la novena versión del sistema operativo móvil de Google: Android 9 o «Pie» por su nombre en código. Como suele ser habitual, **una gran parte de fabricantes aún no han publicado sus nuevas actualizaciones con esta versión.**

A mediados de agosto, se detalla un nuevo tipo de ataque que afecta a los terminales móviles Android, **«Man-in-the-Disk». Este ataque podría poner en peligro aplicaciones legítimas manipulando los datos que éstas procesan en el almacenamiento externo.** Para un ejemplo práctico del ataque se usó el instalador de la versión Android del popular videojuego *Fortnite*. El error fue descubierto por investigadores de Google y publicado tras tan solo siete días (en vez de los 90 días del periodo de gracia otorgado a los fabricantes de forma habitual), **algo que no fue bien recibido por el CEO de Epic Games, Tim Sweeney.** Días antes, Epic Games anunciaba que su videojuego no iba a estar disponible en la Play Store de Google.

Hacia finales de octubre, *The Verge*, publica detalles de un presunto contrato en el que se requiere a los fabricantes que adopten Android que **publiquen actualizaciones de seguridad durante al menos dos años:** un mínimo de cuatro actualizaciones el primer año tras el lanzamiento de un modelo de terminal y el segundo año sin un número determinado de entregas.

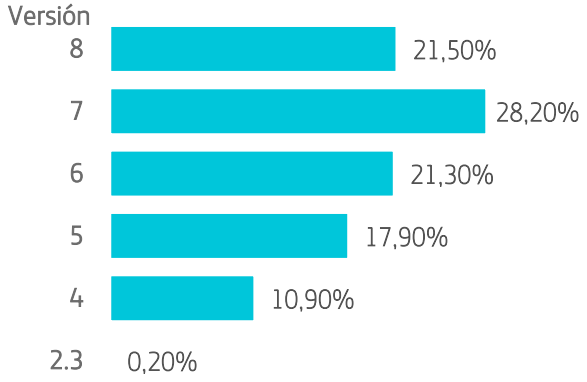
Nuevas características de seguridad[3]

Android 9 trajo las siguientes novedades en materia de seguridad:

- Nuevo **formato de firma para los APK,** con soporte para la rotación de claves.
- Soporte biométrico a través de la API **BiometricPrompt.**
- Nuevas herramientas y contramedidas antiexploit como Control Flow Integrity, que detecta cambios dinámicos en el flujo de ejecución de un binario.
- Actualización del cifrado basado en archivos **(un nivel más granular del cifrado de disco)** para dar soporte al almacenamiento externo.
- Actualización a la versión 4 de Keymaster y mejoras en el cifrado.
- Soporte para el **cifrado de metadatos** (si existe el hardware adecuado)
- Mejoras en el soporte y uso de **SELinux.**

Fragmentación en sistemas Android

Tradicionalmente, **la fragmentación ha sido la gran queja de los desarrolladores de aplicaciones para Android.** Sin olvidar el reducido tiempo de soporte de parches de seguridad. El estado de la fragmentación del sistema operativo móvil de Google, Android, es la siguiente[4]:



Los porcentajes son representativos del número de versión absoluto (es decir, para facilitar su lectura se han sumado las versiones 4.x, por ejemplo).

Los datos arrojan una fragmentación muy marcada. **Gran parte del parque de sistemas operativos Android posee una antigüedad superior a los 2 años.**

Esto supone que **las versiones inferiores a Android 'Nougat' 7, no poseen soporte de actualizaciones.**

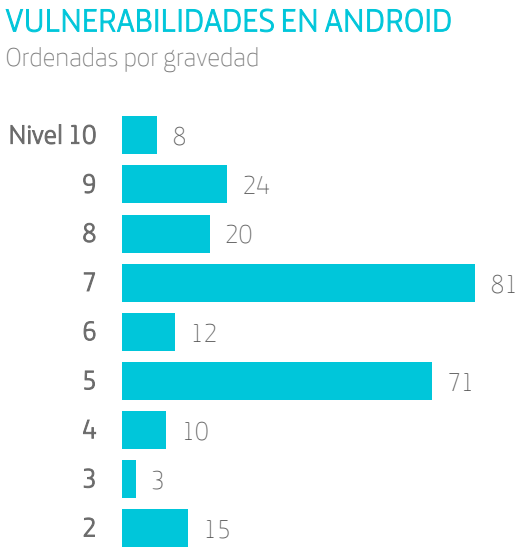
> La última versión de Android ha basado sus mejoras de seguridad en un cifrado más robusto y granular, y en la introducción de mejoras de seguridad antiexploit.

[3] https://source.android.com/setup/start/p-release-notes#security_features

[4] https://developer.android.com/about/dashboards/

Evolución de vulnerabilidades en Android durante el segundo trimestre de 2018

Se han encontrado un total de **173 vulnerabilidades** de diversa gravedad:



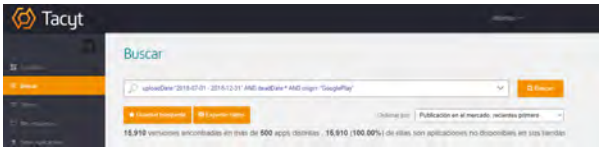
Tiempo medio de retirada de aplicaciones maliciosas en Google Play

Hemos estudiado **el tiempo que tarda Google Play (el market oficial de aplicaciones para Android) en retirar aplicaciones maliciosas (o como es denominado por Google: Potentially Unwanted Application).** Esto es, el tiempo que permanece disponible al público desde que la aplicación es subida por su autor o autores hasta que finalmente es retirada. Los motivos más habituales de retirada del market oficial son:

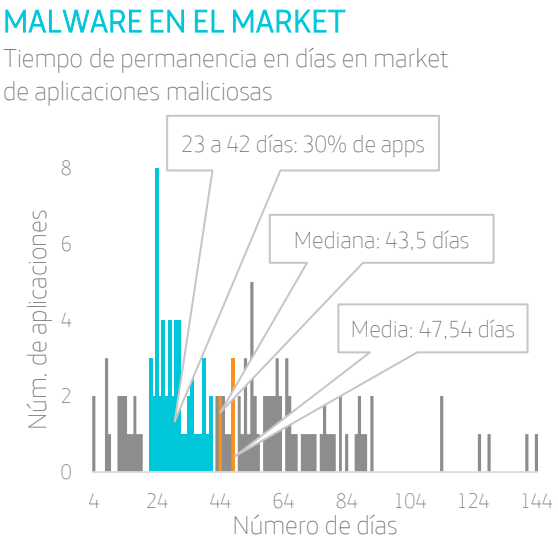
- El propio dueño retira la aplicación.
- Incumple los términos de uso del market en algún aspecto no relacionados con el malware (como, por ejemplo, problemas de copyright)
- Se trata de malware/adware agresivo que rompe igualmente los términos de uso (o *Potentially Unwanted Application*, en terminología de Google).

En este informe hemos querido estudiar **cuál es la capacidad de reacción de Google ante la última circunstancia.** Para ello, no solo se tiene en cuenta que la aplicación haya sido retirada, sino que para contabilizar su "tiempo de vida", **la aplicación debe ser detectada como malware por varios motores antivirus.**

El periodo de estudio comprende desde el 1 de julio de 2018 hasta el 31 de diciembre de 2018. El grueso de aplicaciones seleccionadas es de 15.910 aplicaciones retiradas en algún momento del periodo mencionado:



De ellas, **hemos analizado un subconjunto arbitrario de más de 2.000 aplicaciones y hemos obtenido 142 aplicaciones maliciosas.** Mostramos el número de días hasta su retirada:

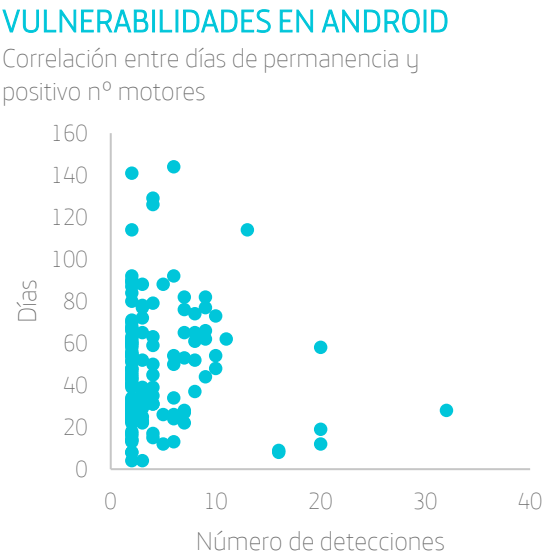


Es interesante destacar que es posible que alguna aplicación no fuese maliciosa o detectada desde el primer momento en el que fue subida, **sino que fuese actualizada con código más agresivo en sucesivas actualizaciones.** En este caso y para este estudio, hemos considerado las que han sido maliciosas desde que fueron subidas al market.

De media, las aplicaciones detectadas por algún motor antivirus pasan más de 47 en el market oficial Google Play antes de ser retiradas.

Correlación entre número de detecciones (por motores) y permanencia en el market

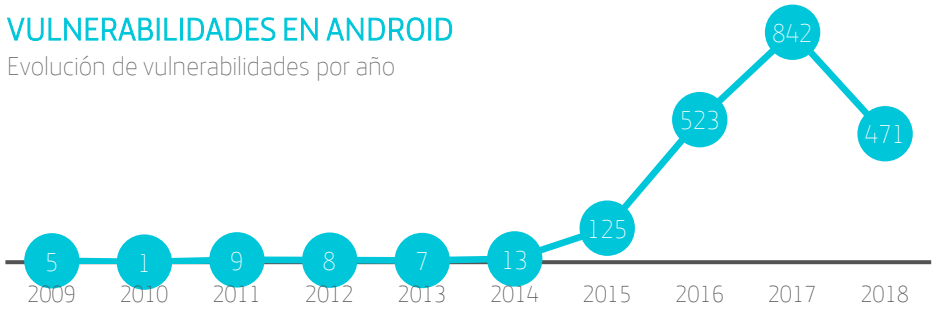
De las tres aplicaciones detectadas por 20 motores, dos fueron retiradas antes de los 20 días, y una aproximadamente a los 60 días.



Las aplicaciones detectadas por menos de 5 motores son las que más aguantan en el market, con apps que se mantienen hasta 100 días. Cuanto más detectadas, menos tiempo en el market, aunque alguna excepción detectada por 20 motores ha estado 60 días disponible para descarga.

Evolución anual por número acumulado de vulnerabilidades

Como se observa, la tendencia o inversión en investigación de vulnerabilidades en el sistema móvil de Google se ha disparado en los últimos tres años.



VULNERABILIDADES

Las vulnerabilidades son en muchos sentidos la piedra angular de la ciberseguridad. Son las responsables de muchos de los ataques y algunas **son tan relevantes que pueden llegar a alterar el ecosistema establecido, poniendo en alerta tanto a atacantes como a defensores,** coordinando a administradores y fabricantes. Es necesario estar atentos a las vulnerabilidades que pueden alterar el equilibrio en la Red. Para comprender la naturaleza de los fallos más comunes en los programas que sostienen la Red es importante conocer cuántas debilidades aparecen y cuáles son las más comunes.

Comentamos en esta sección **algunas de las vulnerabilidades más notables** del segundo semestre de 2018:

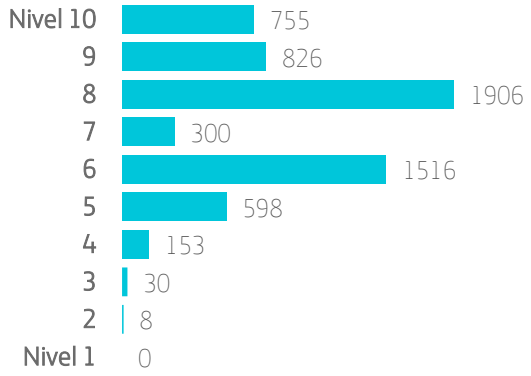
CVE ID	Objetivo	Descripción	Scoring (CVSS v3.0)
CVE-2018-1002105	Kubernetes (Gestor libre de contenedores)	Escalado de privilegios remoto sin necesidad de autenticación.	9,8
CVE-2018-17456	Git (Gestor de versiones)	Ejecución de código arbitrario a través de la clonación recursiva de submodulos.	8,8
CVE-2018-11776	Apache Struts 2 (Framework de aplicaciones web para Java)	Ejecución remota de código arbitrario.	8,1
CVE-2018-8453	Microsoft Windows 7 a 10 y Windows Server 2008 a 2016	Elevación de privilegios a través de win32k.	7,8
CVE-2018-14665	Xorg (Servidor gráfico X11 para sistemas basados en UNIX)	Escalado de privilegios a root.	N/D
CVE-2018-10933	libssh (Librería para el lenguaje C que implementa el protocolo SSH)	Evasión del proceso de autenticación.	9,1

Las vulnerabilidades en cifras

En la siguiente figura, mostramos en números concretos de vulnerabilidades descubiertas (con CVE y gravedad asignados). La distribución de CVE publicados por nivel de riesgo (*scoring* basado en CVSSv3), ha sido la siguiente:

VULNERABILIDADES

Distribución de vulnerabilidades por riesgo



Los programas de recompensa que han implementado las compañías tecnológicas **animan en parte a los investigadores a centrarse en los hallazgos más críticos** (los mejor premiados) en vez de aquellos que no cualifican o su recompensa es mucho menor.

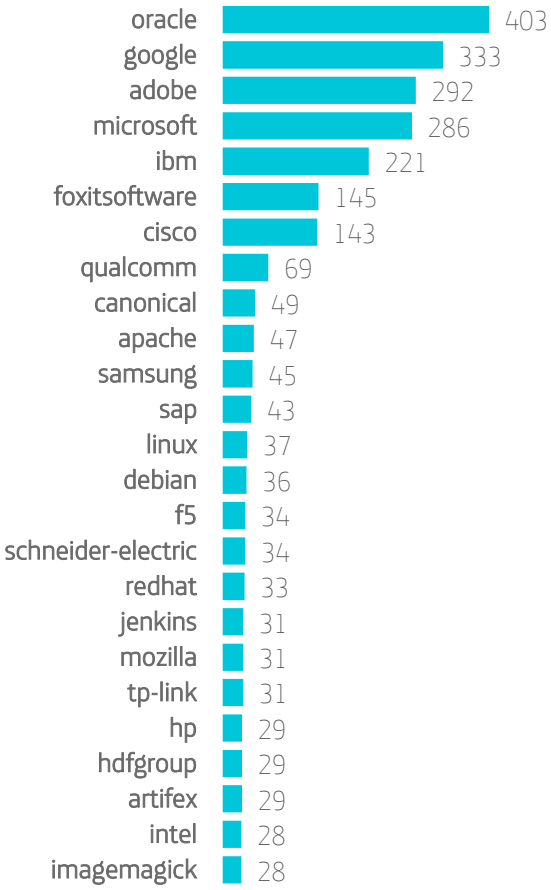
Una prueba del éxito de los programas de recompensa es que Europa financiará a partir de 2019 *Bug Bounties* para 14 proyectos de código abierto muy usados.

Top 25 compañías con más CVE acumulados

Es importante destacar que los números no deben interpretarse de forma absoluta, dado que algunos fabricantes poseen numerosos productos candidatos a recibir un CVE. Por ejemplo, llama la atención la diferencia de Oracle respecto a los demás. Esto puede ser explicado debido **al inmenso catálogo de productos on-premise que Oracle posee.** En contraste, las aplicaciones en la nube de Google no suelen recibir CVE, dado que las vulnerabilidades son corregidas internamente.

VULNERABILIDADES

Top 25 fabricantes por CVE acumulados



Podemos ver una acumulación de vulnerabilidades descubiertas en cierto tipo de software, como, por ejemplo, los **lectores de PDF de Adobe y Foxit** o la librería y conjunto de utilidades ImageMagick, que en los últimos periodos está recibiendo bastante atención a su código por parte de investigadores.

Debian parece ostentar un número bajo para la cantidad de parches que libera para su distribución, **pero solo se tiene en cuenta los productos propios de la organización y no aquellos que mantiene como paquetes de terceros.**

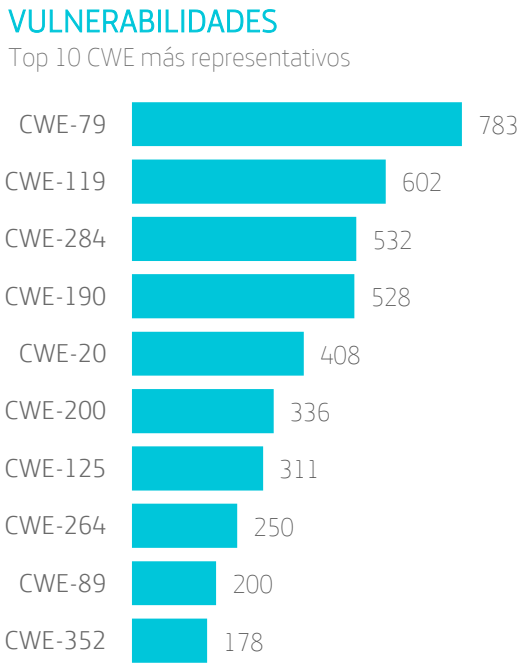
El caso de Adobe merece una atención particular: **casi todos los CVE se corresponden con su software Acrobat Reader, con 239 CVE asignados.** Hace unos años, tanto Flash como Acrobat Reader eran vectores de entrada de malware al ser ejecutados bajo el contexto del navegador, como complementos de éste. Respecto a esta tendencia, desde la inclusión de lectores implementados directamente en JavaScript, como a la práctica desaparición de la tecnología Flash (desplazada por los avances en tecnología web), han hecho que este tipo de productos sean relegados a ser usados de forma ajena al navegador.

No obstante, por ejemplo, la apertura de un PDF adjunto al correo con un visor configurado para usar uno de estos productos, conllevaría la posibilidad de ser infectado si el lector permanece vulnerable. Por lo que aún seguiría siendo un vector a tener en cuenta.

Top 10 CWE más representativos

CWE (Common Weakness Enumeration) es una clasificación que agrupa todas las debilidades identificadas en productos informáticos. Similar al esfuerzo realizado con CVE para etiquetar las vulnerabilidades concretas, halladas por producto, CWE se centra en definir los tipos de forma abstracta. Esto permite realizar un mapeo directo entre CVE y CWE.

Esta lista comprende a **los 10 CWE que más se han asignado por número de CVE.** Esto nos permite observar qué tipo o clase de debilidades han sido más frecuentes en este periodo de estudio.



La siguiente tabla describe cada CWE recogido en el gráfico anterior:

CWE	Titulo	Descripción	Cantidad
CWE-79	Improper Neutralization of Input During Web Page Generation	Básicamente, recoge los tres tipos conocidos de vectores para realizar un Cross-site scripting: Reflejado, almacenado y basado en DOM	783
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	De forma general, recoge aquellos errores de programación donde no se está controlando la capacidad de un buffer de memoria, tanto en operaciones de escritura como de lectura.	602
CWE-284	Improper Access control	La aplicación no restringe el acceso a los recursos de forma adecuada. Se trata de un capítulo genérico donde se recogen aquellos defectos relacionados con la falta de prohibición o control adecuado cuando un tercero accede a recursos para los cuales no posee los permisos adecuados.	532
CWE-190	Integer overflow or Wraparound	Se produce cuando se suma a un entero una cantidad que no puede ser almacenada por su tamaño definido. En ese caso la suma desborda y el resultado puede ser un número inferior al montante original o incluso interpretado como negativo.	528
CWE-20	Improper Input Validation	Categoría general para errores que consisten en un control deficiente o inexistente en entradas de datos procedentes de usuario.	408
CWE-200	Information Exposure	Recoge, de forma general, el compromiso de información sensible debido a la ausencia o deficiencia de controles que impidan la fuga de información.	336
CWE-125	Out-of-bounds Read	Muy relacionada con CWE-119, recoge operaciones de lectura a memoria rebasando los límites de control de un búfer en concreto.	311
CWE-264	Permissions, Privileges and Access Controls	Se trata de una categoría general donde entra toda deficiencia relacionada con los permisos atribuidos a los usuarios o procesos, los privilegios que se les atribuye y el control de acceso a los recursos (relacionada, en este sentido, con CWE-284).	250
CWE-89	Improper Neutralization of Special Elements used in a SQL Command	Relacionada con CWE-20, pero especializada en código SQL. La aplicación es incapaz de filtrar adecuadamente las cadenas de datos procedentes de usuario provocando el acceso no controlado a la base de datos.	200
CWE-352	Cross-site Request Forgery (CSRF)	Ausencia o deficiencia en mecanismos que permitan discernir si una petición web proviene de una acción consciente del usuario autenticado o por el contrario, dicha acción ha sido iniciada por un tercero en el contexto de la sesión activa de un usuario.	178

Podríamos clasificar los fallos más comunes en tres tipos de forma muy general:

- **Ausencia de controles adecuados** que vigilen por una correcta autenticación, autorización y seguimiento del uso los privilegios otorgados; la conocida como triada AAA (Authentication, Authorization and Accountability).
- **Falta de filtrado seguro** de los datos que provienen de usuario.
- Errores en la **gestión de memoria dinámica.**

No existe un desplazamiento significativo respecto a un tipo general u otro. Los errores clasificados mantienen cifras similares cuando son agrupados en estas tres categorías. Por ejemplo, los tres primeros CWE de la clasificación albergan cifras muy cercanas y perfilan adecuadamente la clasificación señalada.

La ausencia de controles respecto a la triada AAA pertenece a todo rango de aplicaciones, aunque se da más en aquellas que mantienen una jerarquía de usuarios con sus respectivos permisos y privilegios, por ejemplo, sistemas operativos y aplicaciones web.

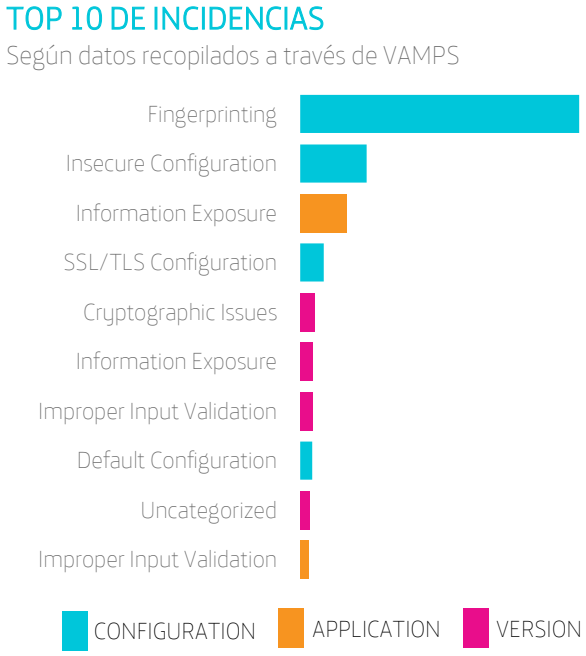
La segunda categoría está estrechamente relacionada, sobre todo, con aplicaciones web donde la entrada de usuario puede provocar distintos efectos nocivos sin no se controla: Cross-site scripting, inyecciones SQL, inyecciones que causan ejecución de comandos, inclusión de archivos locales o remotos, etc.

La tercera categoría excluye casi completamente a las aplicaciones web, dado que la gestión de memoria está asociada a sistemas operativos y código nativo.

Con diferencia, según nuestros sistemas de monitorización a clientes, los problemas de seguridad más frecuentes están relacionados con la configuración de las aplicaciones y servicios, seguidos de problemas de versiones anteriores.

Top 10 de fallos más comunes y sus consecuencias según VAMPS

A continuación, se ofrece una lista de los 10 errores más comunes (por número de incidencias) reportados sobre nuestros clientes gracias a VAMPS.



En contraste con la información de apartados anteriores, **estos datos reflejan el día a día de sistemas en funcionamiento y son auditados con periodicidad.** Los errores más comunes siguen siendo aquellos que se derivan de un descuido o atribuidos a un despliegue incorrecto. La mayoría de las entradas reflejan una necesidad de aplicación de políticas de seguridad que contengan, tanto las instrucciones concretas para realizar un despliegue seguro, como los controles que ayuden a detectar y corregir las deficiencias o incumplimientos de la política de seguridad. Por ejemplo, archivos olvidados pero accesibles (tanto de configuración como documentales) de los que se puede obtener información sensible. En el apartado de configuración insegura, podemos incluir la falta de actualización TLS, o carencia de cabeceras que prevengan otro tipo de ataques.

OPERACIONES APT, GRUPOS ORGANIZADOS Y MALWARE ASOCIADO

Repasamos la actividad de los distintos grupos a los que se les atribuye la autoría de operaciones APT o campañas reseñables. Como se ha demostrado en muchas ocasiones, **la atribución de este tipo de operaciones, así como la composición, origen e ideología de los grupos organizados, es compleja y por definición, no puede ser completamente fiable.** Los actores pueden utilizar (y utilizan) medios para manipular la información de modo que oculte su verdadero origen e intenciones. Es ya habitual que en determinados casos usurpen el modus operandi de otros grupos para desviar la atención o perjudicar a estos últimos.

Operaciones APT detectadas durante el segundo semestre de 2018

Campaña	Publicación	Grupo	Malware	Objetivos	Notas
GOLDFIN	Accenture (agosto 2018, se cree activa desde febrero de 2017)	CANDLEFISH (Patchwork, Dropping Elephant, Chinastrats)	SOCKSBOT	Instituciones financieras de la Comunidad de Estados Independientes	• Empleo de *spear phishing* • Infraestructura coincidente con grupo FIN7, además de coincidencia de técnicas de ofuscación para el código en PowerShell
GlanceLove	Check Point Research (julio 2018, se cree activa desde noviembre de 2017)	Inteligencia militar israelí sostiene que la campaña estaría organizada por *Hamas*	Varias aplicaciones Android dentro del market oficial GooglePlay	Militares israelíes	• Phishing usando motivos de la Copa del Mundo FIFA 2018 • Robo de credenciales de navegadores y gestores de correo, imágenes, contactos, etc. • Malware modular con componentes especializados
LeafMiner	Symantec (julio 2018)	LeafMiner		Empresas de Oriente Medio	• Empleo y modificación de exploits públicos (Fuzzbunch framework, Eternal Blue...) • Uso de técnicas como Watering Hole
Operation DOOS (verano de 2017)	Area 1	OilRig (IRN2)	Helminth	Empresas de Gas y Petróleo de Oriente Medio	• Empleo de PowerShell y VBScript • Empleo de *phishing* • Uso de documentos Excel con macros maliciosas
Operation Red Signature (julio de 2018)	TrendLabs (agosto 2018)	Desconocido	9002 RAT	Organizaciones de Corea del Sur	• Explotación de CVE-2017-7269 • Volcado de credenciales de bases de datos
Operation Red Signature (julio de 2018)	FireEye (julio 2018)	TEMP.Periscope (China)	EVILTECH, DADBOB	Gobierno y personalidades de Camboya (además de otras regiones EEUU, Europa y Oriente Medio)	

Nuevos grupos organizados detectados durante el segundo semestre de 2018

Grupo	Origen	Publicación	Objetivos	Notas
DARKHYDRUS		PaloAlto Networks -UNIT42 (julio de 2018)	Agencias gubernamentales de Oriente Medio	• Empleo de *spear phishing* • Empleo de dominios como: micrrosoft[.]net, cisc0[.]net, 0utl00k[.]net, allexa[.]net y otros similares.
Gordon Group	Posiblemente Pakistan	PaloAlto Networks -UNIT42 (agosto de 2018)	No definidas. Actuaciones detectadas en Reino Unido, España, Rusia y Estados Unidos, entre otras muchas	• Uso de acortadores de URL para descarga de payloads • Uso de múltiples documentos office maliciosos, con macros y empleo de PowerShell

Malware asociado a operaciones APT activas o descubiertos durante el segundo semestre de 2018

Malware	Grupo	Origen	Objetivos	Publicación	Notas
QUADAGENT	OilRig (APT34, Helix Kitten)	Presumiblemente, Oriente Medio	Principalmente, Oriente Medio y otros	PaloAlto Networks - UNIT42 (julio de 2018)	• Vector: macro maliciosa en documento ofimático. • Uso de .Net y PowerShell • Empleo de tácticas *spear phishing* • Uso de código público: https://github.com/danielbohannon/Invoke-Obfuscation
BISKVIT	No identificado	Desconocido	Posiblemente, personal militar ruso	Fortinet (agosto de 2018)	• Malware escrito para .Net • Empleo de phishing (Correo en idioma ruso de temática militar) • Explota CVE-2017-0199 (ligado a operaciones anteriores)
Final1stspy	APT37, Group123, Reaper	Corea del Norte	Probables, Oriente Medio y Sureste asiático	INTEZER (octubre de 2018)	• Comparte código e infraestructura con malware ROKRAT, NOKKI, KONN, entre otros

El empleo de *spear phishing* y documentos ofimáticos maliciosos (principalmente a través de macros) es la fórmula de infección más común entre los grupos estudiados, tanto los nuevos como reincidentes e independientemente de su origen.

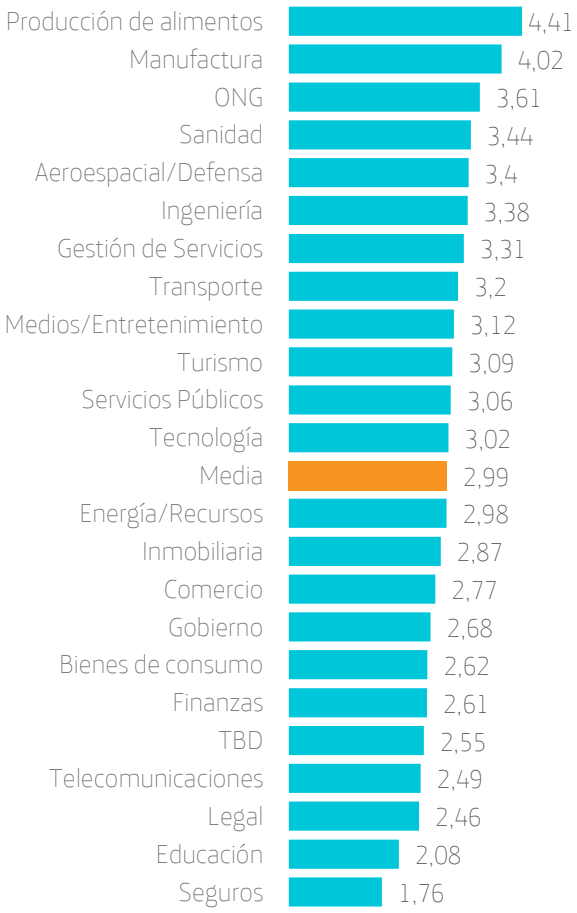
EVALUACIÓN DEL CIBERRIESGO POR SECTORES

Para establecer una comparativa de seguridad entre industrias, utilizamos la tecnología de BitSight y su Security Rating Platform.

BitSight genera medidas objetivas y cuantitativas sobre el rendimiento de la seguridad de una empresa, evaluada diariamente. No se monitorizan las políticas, leyes o buenas prácticas ni se analizan análisis de red. **Se incluyen incidentes, evidencias externas (por ejemplo, conexiones a panel de control desde una IP que pertenece a la compañía, leaks en redes sociales, ...) y otros datos que, gracias a los algoritmos de BitSight, permiten ofrecer una idea muy aproximada de la seguridad en una compañía,** incluyendo incluso sus proveedores tecnológicos. Esto implica una de las evaluaciones más exactas sobre el riesgo en ciberseguridad. Los datos se dividen en cuatro clases: sistemas comprometidos, diligencia, comportamiento del usuario, y revelaciones públicas.

Con esta tecnología, hemos conseguido **destilar información muy relevante sobre las prácticas de seguridad de los sectores industriales en Europa** y comparado con España, como en el siguiente ejemplo.

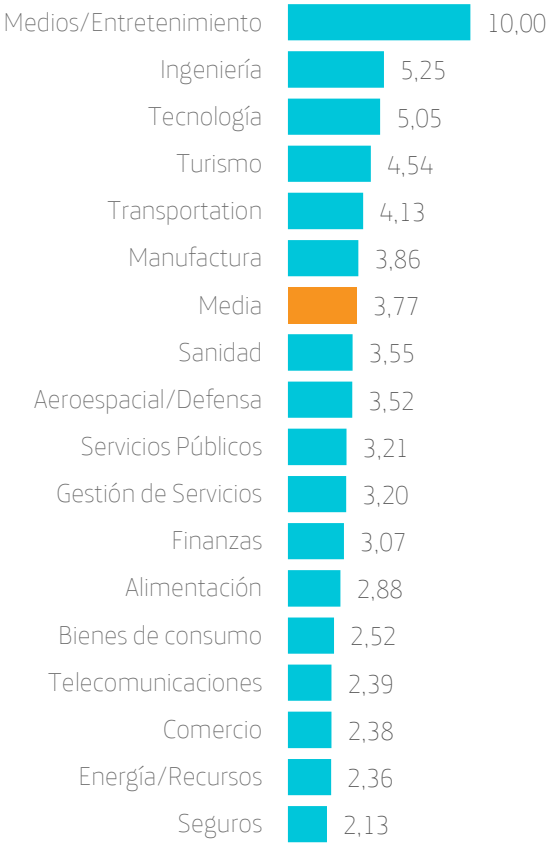
Número medio de días efectivos que necesita una compañía europea para solucionar una amenaza de malware, agrupado por sector.



Las compañías de producción de alimentos europeas tardan una media de 4,41 días en solucionar sus problemas de malware, mientras que las compañías de seguros apenas llegan a las 48 horas.

Si nos centramos en España, la media es la siguiente:

Días desde la detección hasta la neutralización de la amenaza en España, por sectores

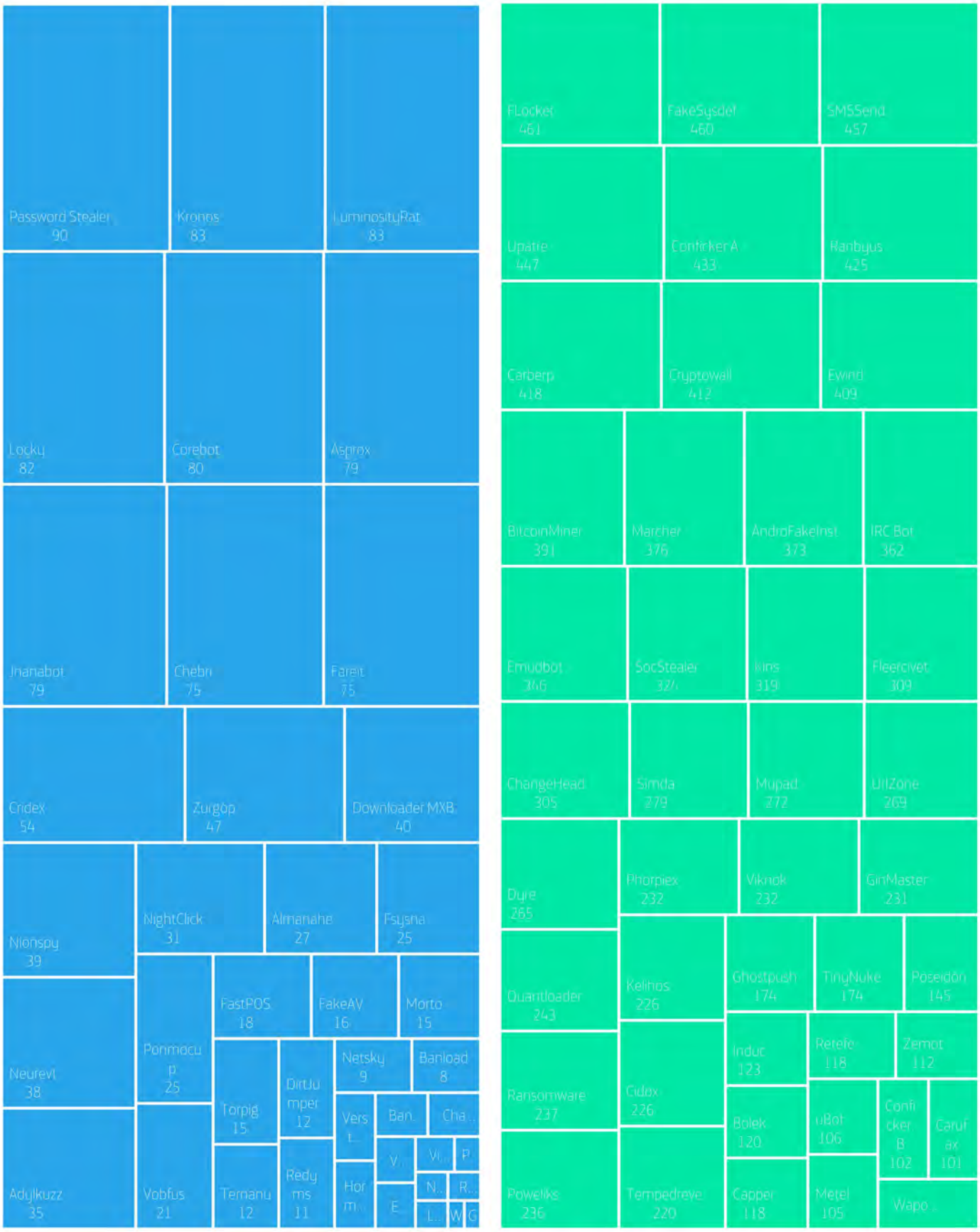


Se puede comprobar **que la media española (3,77 días) es superior a la europea.**

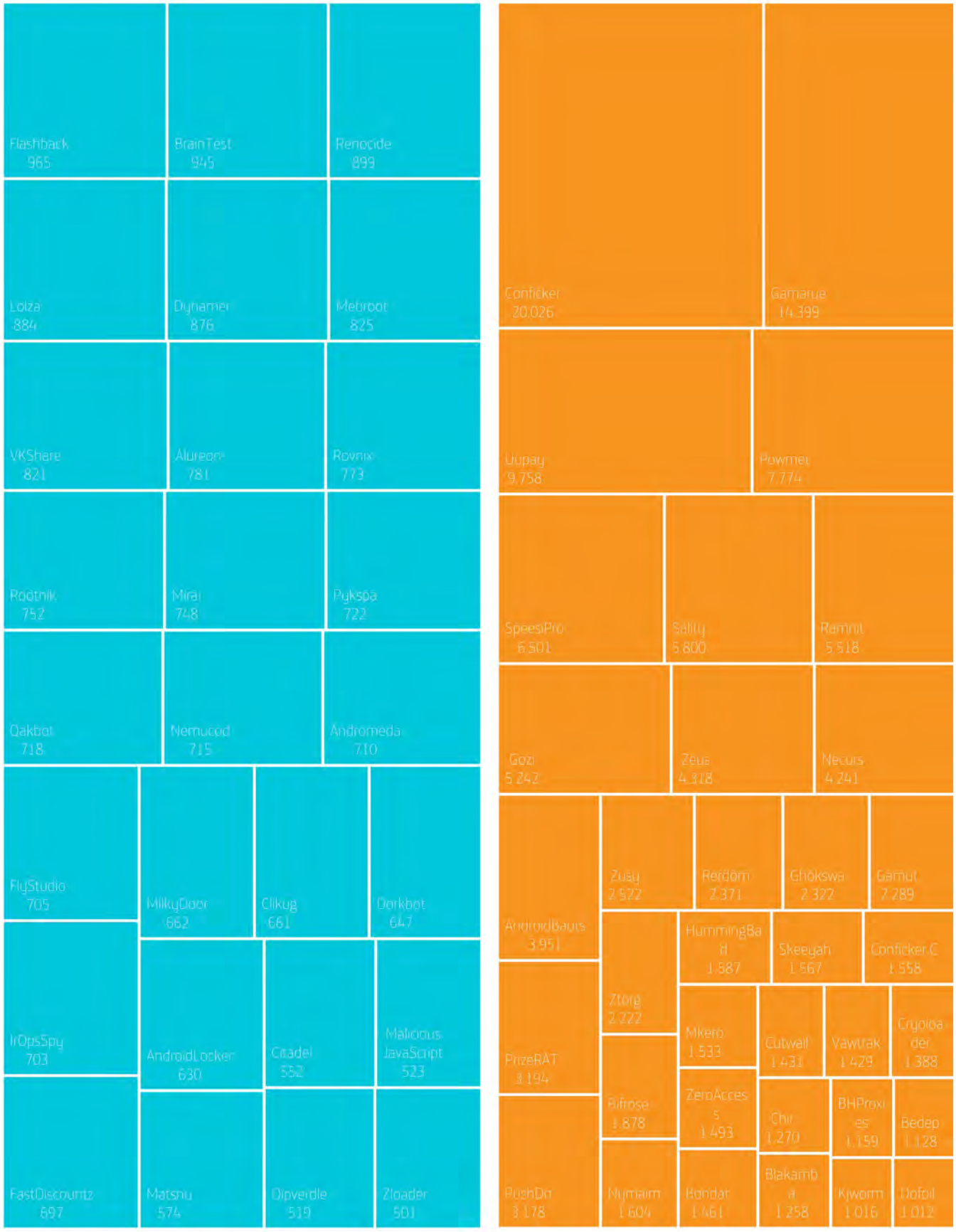
Gracias a la tecnología de BitSight, **también podemos saber qué familias de malware e infecciones han sido más detectadas en Europa y España.**

La tecnología Bitsight ofrece una visión muy innovadora sobre el ciberriesgo asociado a una compañía. Se basa en sistemas comprometidos, diligencia, comportamiento del usuario, y revelaciones públicas. En estas métricas, agrupadas por sectores en Europa, analizamos la celeridad para solucionar incidentes, y además qué malware es el más común en sus infraestructuras.

Los siguientes gráficos describen el nombre de la familia a la que pertenece la muestra detectada y el número de infecciones o prevalencia durante estos últimos meses.



0 INFECCIONES 100 500



1.000 INFECCIONES 20.000

RECAPITULACIÓN

- Durante los últimos 6 meses del año, se han publicado 125 vulnerabilidades en iOS, **el 56% con una gravedad de 7 sobre 10 o superior.** Con esto acumula 1496 vulnerabilidades desde 2007.
- Durante el mismo periodo se han publicado 173 vulnerabilidades en Android, **el 18% con una gravedad de 7 sobre 10 o superior.** Con esto acumula 1950 vulnerabilidades desde 2009.
- Aproximadamente **una tercera parte de las apps maliciosas detectadas en Google Play, permanecen entre 22 y 42 días en el market.** La media total de permanencia de aplicaciones maliciosas es de 47,45 días.
- **El 11% de los iPhone ejecutan un iOS anterior al 11.** En el caso de Android, la mitad de los existentes ejecutan una versión no soportada ya.
- Hemos analizado 3.528 vulnerabilidades en estos seis meses. **El 65% tienen una gravedad de 7 ó superior.** Oracle, Adobe y Microsoft son los fabricantes con más CVEs asignados.
- La mayoría de los problemas de seguridad detectados en nuestros clientes son **fugas de información por ficheros sensibles o metadatos, y la pobre implementación de cabeceras HTTP** para proteger de ataques.
- El empleo de *spear phishing* y documentos ofimáticos maliciosos (principalmente a través de macros) **es la fórmula de infección más común** entre los grupos de atacantes más sofisticados.
- Una compañía europea **necesita una media de casi 3 días para solucionar una amenaza de malware. Los más rápidos son el sector Seguros (con menos de dos días) y los más lentos, el sector de la Alimentación,** con más de 4 días.
- En España, **la industria del entretenimiento necesita hasta 10 días para neutralizar una amenaza por malware.**
- **Gamarue y Conficker siguen siendo las amenazas de malware más populares** en Europa.

Acerca de ElevenPaths

En ElevenPaths, la Unidad de Ciberseguridad de Telefónica, creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre la seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y de esta manera, ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Más información

www.elevenpaths.com
@ElevenPaths
blog.elevenpaths.com