Eleven Paths

Informe sobre el estado de la seguridad 2019 H2

Desde la seguridad en móviles hasta el ciberriesgo, desde las noticias más relevantes hasta las más técnicas y las vulnerabilidades más habituales, comprende los riesgos del panorama actual

elevenpaths.com

Telefónica CYBER SECURITY UNIT

ÍNDICE

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), adoptando 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.

Durante el segundo semestre de 2019, los protagonistas han sido de nuevo algunos ataques de ransomware destacables. Muy probablemente gracias a Emotet, que volvió a la carga a finales de año con fuerza. Si bien Emotet es el vector de entrada más común, existen otros muchos más complejos para realizar ataques más selectivos. A principios de octubre, se descubrió un grave fallo en WhatsApp con ciertas particularidades. Se originaba en una librería de código abierto de tratamiento de GIFs explotable al abrir la galería de WhatsApp. Y la ejecución heredaría todos los permisos de la aplicación vulnerable. Más tarde WhatsApp sufriría otro grave problema de seguridad que permitía la ejecución de código en cualquier plataforma con solo enviar un archivo MP4. A raíz de estos fallos y por tener constancia de que estaban siendo usados contra víctimas muy concretas, Facebook demandó a la NSO por atentar contra sus usuarios.

Y hablando de espionaje, este semestre también hemos sabido que desde mayo a diciembre de 2015 (cuando abandonaron la compañía) dos empleados de Twitter (Ahmad Abouammo y Ali Alzabarah) estaban al servicio de Arabia Saudí para espiar a disidentes en la plataforma. Había sido reclutados en 2014 y accedieron a datos privados de más de 6000 cuentas. IP, números de teléfono, dispositivos usados... Todo lo que podían sacar de una cuenta de alguien interesante para el gobierno les era proporcionado por los trabajadores internos gracias a su posición. Incluso llegaban a cerrar cuentas de disidentes a requerimiento gubernamental.

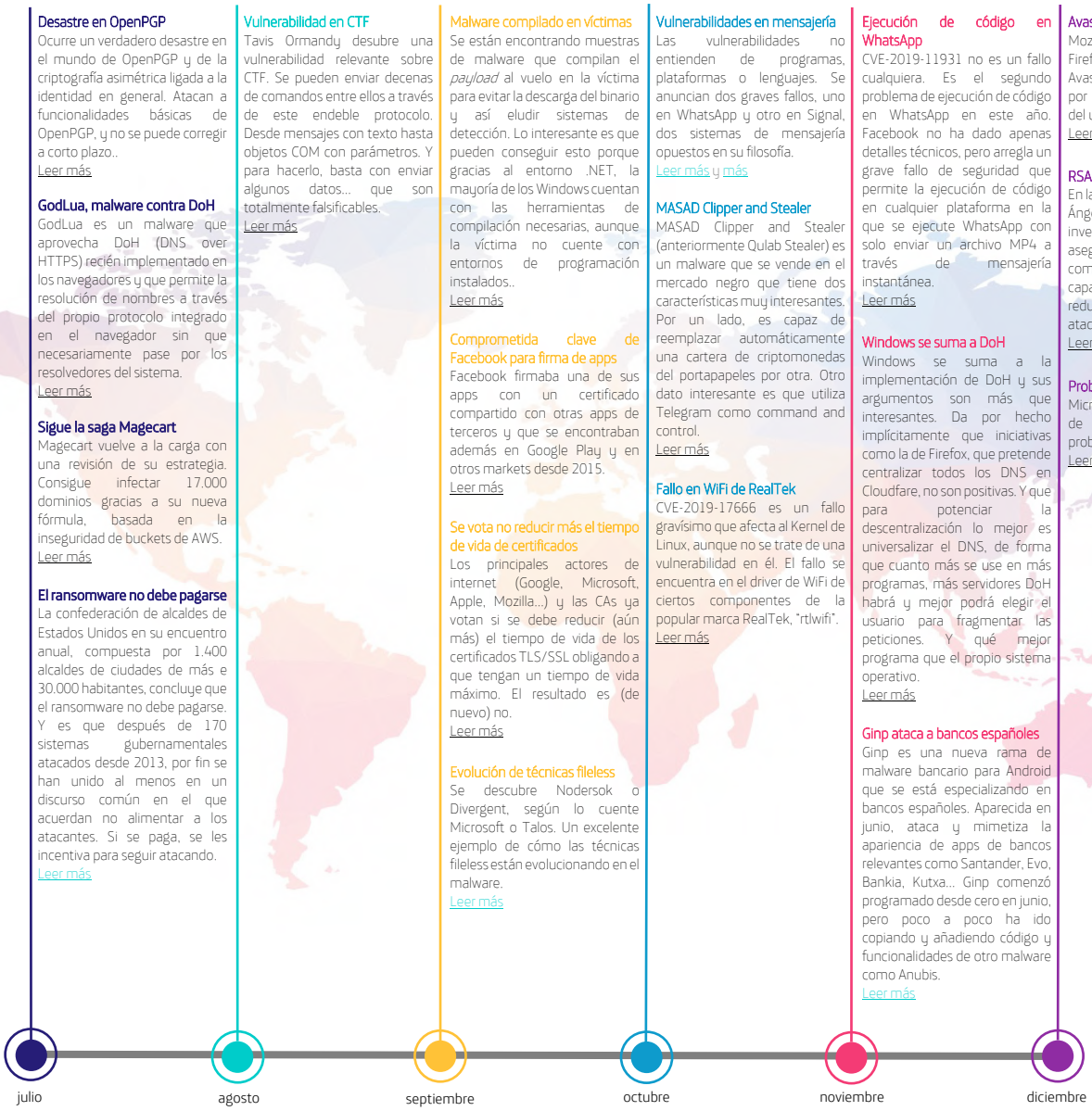
Precisamente para mejorar la privacidad, este semestre ha sido sin duda cuando tanto Firefox como Chrome han apostado por DNS over HTTPS (DOH) más en serio, poniendo en marcha dos fórmulas diferentes para su adopción. Firefox más agresivo, Chrome más compresivo con las necesidades de los ISP.

Por otro lado, este semestre el grupo Magecart ha seguido innovando en sus ataques. Atacaron tanto webs menores como algunas más relevantes. En un ligero cambio de estrategia, en algunos casos los ataques se realizaban después de introducir los datos de envío. Ese era el momento en que las víctimas eran redirigidos a un sitio falso donde introducir sus datos de la tarjeta de crédito. Luego volvían a lugar real que les pedía (ahora de forma legítima) los datos de la tarjeta.

Tanto si se es aficionado como profesional, es importante ser capaz de seguir el ritmo de las noticias relevantes sobre ciberseguridad: ¿qué es lo más relevante que está pasando? ¿Cuál es el panorama actual? El lector dispondrá con este informe 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.

LOS INCIDENTES MÁS DESTACADOS DEL SEGUNDO SEMESTRE DE 2019

A continuación, damos cuenta de aquellas noticias que mayor impacto han tenido durante el transcurso de este segundo semestre de 2019.



Desastre en OpenPGP
Ocurre un verdadero desastre en el mundo de OpenPGP y de la criptografía asimétrica ligada a la identidad en general. Atacan a funcionalidades básicas de OpenPGP, y no se puede corregir a corto plazo..
Leer más

GodLua, malware contra DoH
GodLua es un malware que aprovecha DoH (DNS over HTTPS) recién implementado en los navegadores y que permite la resolución de nombres a través del propio protocolo integrado en el navegador sin que necesariamente pase por los resolvedores del sistema.
Leer más

Sigue la saga Magecart
Magecart vuelve a la carga con una revisión de su estrategia. Consigue infectar 17.000 dominios gracias a su nueva fórmula, basada en la inseguridad de buckets de AWS.
Leer más

El ransomware no debe pagarse
La confederación de alcaldes de Estados Unidos en su encuentro anual, compuesta por 1.400 alcaldes de ciudades de más e 30.000 habitantes, concluye que el ransomware no debe pagarse. Y es que después de 170 sistemas gubernamentales atacados desde 2013, por fin se han unido al menos en un discurso común en el que acuerdan no alimentar a los atacantes. Si se paga, se les incentiva para seguir atacando.
Leer más

Vulnerabilidad en CTF
Tavis Ormandy desubre una vulnerabilidad relevante sobre CTF. Se pueden enviar decenas de comandos entre ellos a través de este endeble protocolo. Desde mensajes con texto hasta objetos COM con parámetros. Y para hacerlo, basta con enviar algunos datos... que son totalmente falsificables.
Leer más

Malware compilado en víctimas
Se están encontrando muestras de malware que compilan el *payload* al vuelo en la víctima para evitar la descarga del binario y así eludir sistemas de detección. Lo interesante es que pueden conseguir esto porque gracias al entorno .NET, la mayoría de los Windows cuentan con las herramientas de compilación necesarias, aunque la víctima no cuente con entornos de programación instalados..
Leer más

Comprometida clave de Facebook para firma de apps
Facebook firmaba una de sus apps con un certificado compartido con otras apps de terceros y que se encontraban además en Google Play y en otros markets desde 2015.
Leer más

Se vota no reducir más el tiempo de vida de certificados
Los principales actores de internet (Google, Microsoft, Apple, Mozilla...) y las CAs ya votan si se debe reducir (aún más) el tiempo de vida de los certificados TLS/SSL obligando a que tengan un tiempo de vida máximo. El resultado es (de nuevo) no.
Leer más

Evolución de técnicas fileless
Se descubre Nodersok o Divergent, según lo cuente Microsoft o Talos. Un excelente ejemplo de cómo las técnicas fileless están evolucionando en el malware.
Leer más

Vulnerabilidades en mensajería
Las vulnerabilidades no entienden de programas, plataformas o lenguajes. Se anuncian dos graves fallos, uno en WhatsApp y otro en Signal, dos sistemas de mensajería opuestos en su filosofía.
Leer más y más

MASAD Clipper and Stealer
MASAD Clipper and Stealer (anteriormente Qulab Stealer) es un malware que se vende en el mercado negro que tiene dos características muy interesantes. Por un lado, es capaz de reemplazar automáticamente una cartera de criptomonedas del portapapeles por otra. Otro dato interesante es que utiliza Telegram como command and control.
Leer más

Fallo en WiFi de RealTek
CVE-2019-17666 es un fallo gravísimo que afecta al Kernel de Linux, aunque no se trate de una vulnerabilidad en él. El fallo se encuentra en el driver de WiFi de ciertos componentes de la popular marca RealTek, "rtlwifi".
Leer más

Ejecución de código en WhatsApp
CVE-2019-11931 no es un fallo cualquiera. Es el segundo problema de ejecución de código en WhatsApp en este año. Facebook no ha dado apenas detalles técnicos, pero arregla un grave fallo de seguridad que permite la ejecución de código en cualquier plataforma en la que se ejecute WhatsApp con solo enviar un archivo MP4 a través de mensajería instantánea.
Leer más

Windows se suma a DoH
Windows se suma a la implementación de DoH y sus argumentos son más que interesantes. Da por hecho implícitamente que iniciativas como la de Firefox, que pretende centralizar todos los DNS en Cloudfare, no son positivas. Y que para potenciar la descentralización lo mejor es universalizar el DNS, de forma que cuanto más se use en más programas, más servidores DoH habrá y mejor podrá elegir el usuario para fragmentar las peticiones. Y qué mejor programa que el propio sistema operativo.
Leer más

Ginp ataca a bancos españoles
Ginp es una nueva rama de malware bancario para Android que se está especializando en bancos españoles. Aparecida en junio, ataca y mimetiza la apariencia de apps de bancos relevantes como Santander, Evo, Bankia, Kutxa... Ginp comenzó programado desde cero en junio, pero poco a poco ha ido copiando y añadiendo código y funcionalidades de otro malware como Anubis.
Leer más

Avast te espía
Mozilla retira de su navegador Firefox cuatro extensiones de Avast (y AVG, que le pertenece) por atentar contra la privacidad del usuario.
Leer más

RSA contra las cuerdas
En la First IEEE Conference de Los Ángeles presentan una investigación en la que aseguraban que se podían comprometer las claves RSA con capacidades computacionales reducidas. Utilizan el conocido ataque del Batch GCD.
Leer más

Problema en SharePoint
Microsoft saca un parche fuera de ciclo para corregir un problema en SharePoint.
Leer más

MÓVILES

Apple iOS

Noticias destacables

Tal y como anunciábamos en la pasada edición, Apple liberó finalmente la versión 13 de su sistema operativo iOS el 19 de septiembre. Tres meses después de que fuese anunciada (el 3 de junio) durante la conferencia anual de desarrolladores WWDC.

Sin embargo, si hay una noticia destacable, es que a partir de ahora los dispositivos **iPad tendrán su propio sistema operativo independiente** (aunque se trata de un derivado de iOS), denominado iPadOS.

En esta versión, Apple se ha enfocado en la privacidad del usuario. Respecto a las novedades de seguridad, señalamos dos de las más destacables que trae iOS 13. Es algo que notarán los usuarios que actualicen a la nueva versión y una aplicación intente hacer uso del Bluetooth: aparecerá una notificación del sistema preguntando al usuario si autoriza su uso.

Esto evita que el usuario sea seguido a través de dispositivos denominados *Bluetooth beacons*. Se trata de pequeños emisores que son instalados en sitios abiertos al público (habitualmente, tiendas) para, a través de la recepción de un código único, determinar cuándo y cuánto tiempo permanece un usuario en un establecimiento. Una forma sutil de geolocalizar usuarios y hacer un seguimiento de sus hábitos de compra.

Otro hito reseñable es la puesta en público de Apple ID, con opciones de no compartir la cuenta de correo del usuario. En tal caso, **Apple creará una cuenta de correo proxy para evitar exponer la del propio usuario.**

Aun con la versión 13 recién estrenada, se publicó una gran actualización para la versión 12 de iOS (iOS 13 solo está disponible para iPhone 6S o superior), **en concreto la 12.4 que corrige casi 40 fallos de seguridad en diversos componentes.** Algunos de los fallos podrían permitir la ejecución de código en componentes tales como WebKit (afecta de lleno a Safari) y Core Data.

A finales de agosto, Apple publicaría una revisión, la 12.4.1, para parchear un error en el kernel que posibilitaría la ejecución de código arbitrario. Una actualización de emergencia, fuera del ciclo corriente de parches. Tras esta actualización, la rama 12.4 recibió tres nuevas revisiones, la 12.4.2, 12.4.3 y 12.4.4, en septiembre, octubre y diciembre respectivamente. De nuevo corrigiendo, de manera puntual, vulnerabilidades graves en forma de ejecución de código arbitrario. Sin embargo, como curiosidad, no se tienen detalles del boletín correspondiente a la versión 12.4.3.

No tardó mucho la versión 13 en convocar una nueva actualización **a tan solo cinco días de su salida.** Justo el 24 de septiembre se publicaba la 13.1 que corregía más de 20 vulnerabilidades, algunas de ellas consideradas de gravedad alta. **También se incluía un parche para un tipo vulnerabilidad clásico: acceder a ciertas funciones del sistema e información desde la pantalla bloqueada**. En esta ocasión, poder ver los contactos de la agenda a través de VoiceOver.

De nuevo, 48 horas más tarde se publicaba un boletín que incrementaba la versión a la 13.1.1. Esta vez, sin embargo, se trataba de un fallo funcional en las restricciones de la funcionalidad de "Zona protegida", que no eran convenientemente aplicadas a ciertas extensiones de aplicaciones de terceros.

Un mes más tarde **vio la luz la 13.2 con casi 30 CVEs parcheados.** Una gran actualización que cubría numerosos componentes, entre ellos, WebKit y el propio kernel del sistema. Le siguieron a esta actualización los parches 13.2.2 y 13.2.3, pero sin ningún informe de vulnerabilidades de seguridad.

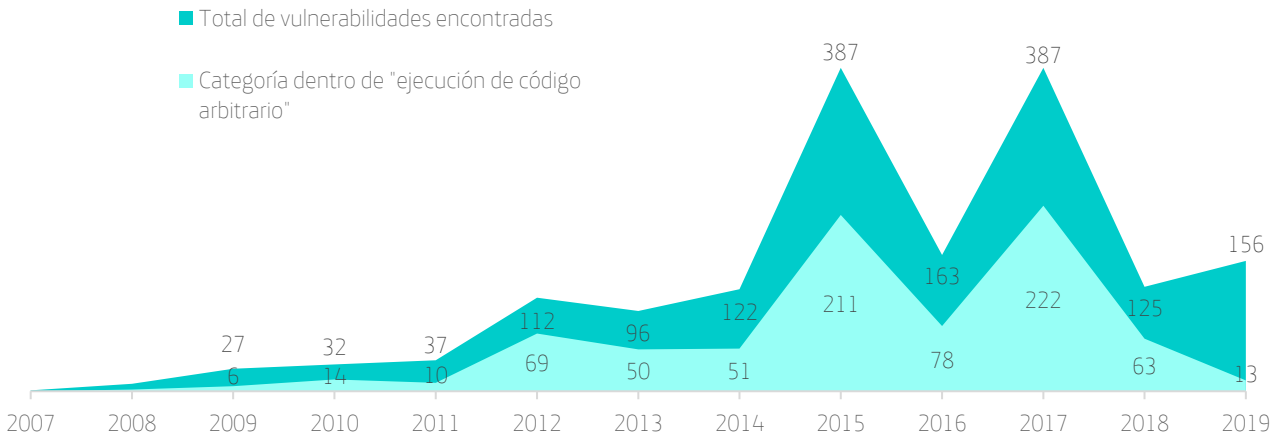
Por último, cerrando este informe, el 10 de diciembre se publica iOS 13.3 con casi 15 parches, más de la mitad de las vulnerabilidades corregidas permitían ejecutar código arbitrario..

Evolución de vulnerabilidades en iOS durante el segundo semestre de 2019

Curiosamente, en los años 2015 y 2017 el número de vulnerabilidades fue el mismo, 387.

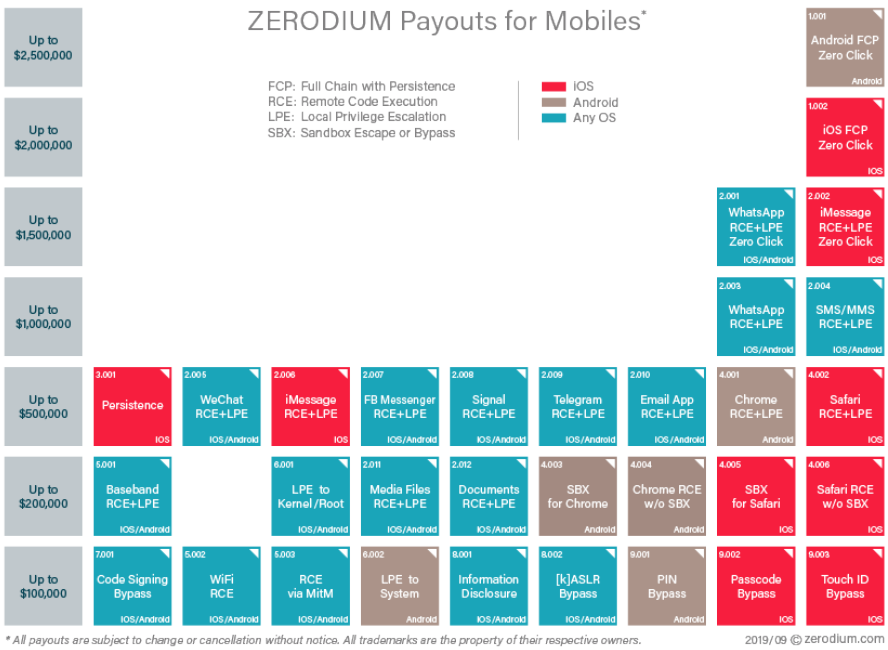
VULNERABILIDADES EN IOS 2019-H2

Evolución de vulnerabilidades por año



En total, **se han parcheado 198 CVE en el pasado semestre.** De los cuales, 13 poseen la categoría de críticos y 6 de ellos permiten la ejecución de código arbitrario. Las cifras representan un aumento respecto del semestre anterior, superando así los periodos anteriores.

Recordemos que un exploit que permita comprometer por completo un dispositivo de la marca Apple se cotiza públicamente en 2 millones de dólares. Según el programa de compra de exploits de la compañía Zerodium.

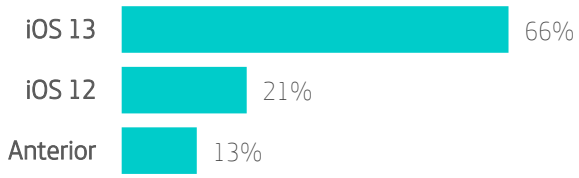


Fragmentación de versiones durante el segundo semestres de 2019

Como podemos observar de los datos de fragmentación en este semestre, **la adopción de la versión actual de iOS es del 66%.** Solo un parque de algo más del 12% son instalaciones de versiones anteriores a la 12 y 13 (sobre todo iOS 11 y 10).

FRAGMENTACIÓN EN APPLE IOS 2019-H2

Según datos de la App Store



El dispositivo más antiguo que soporta la versión 13 es el iPhone 6S, mientras que la versión 12 es soportada por, como mínimo, el iPhone 5S. Dado que este último dispositivo vio la luz en septiembre de 2013, la mayoría del parque de dispositivos de Apple posee menos de siete años y más de la mitad de estos, cinco o menos años.

Como ya hemos comentado en ediciones anteriores, iOS no posee problemas, o al menos estos son menores, cuando se trata de fragmentación de versiones. Los usuarios de Apple experimentan mayores plazos de soporte en los dispositivos. Incluso cuando el sistema operativo cambia en el plazo de poco más de un año, se suelen soportar versiones relativamente antiguas de iPhone. Esto, favorece enormemente la difusión de una nueva versión de iOS y el reemplazo de antiguas versiones.

Informe de Transparencia de Apple

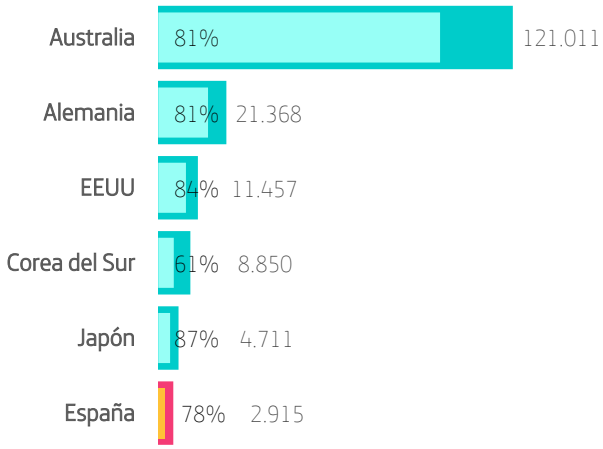
En ocasiones, los gobiernos necesitan apoyarse en las grandes corporaciones para poder llevar a cabo su trabajo. Cuando una amenaza pasa por conocer la identidad o tener acceso a los datos de un potencial atacante o de una víctima en peligro, la información digital que almacenan estas empresas puede resultar vital para la investigación y evitar una catástrofe. Apple publica semestralmente un completo informe sobre qué datos le piden los gobiernos, cuáles y en qué medida las peticiones se satisfacen. Repasamos aquí algunos datos que hemos recopilado sobre las actividades y peticiones de los gobiernos a la compañía.

Peticiones basadas en dispositivos

Representa **peticiones de agencias gubernamentales solicitando información de dispositivos Apple, como número de serie o número IMEI**. Por ejemplo, cuando las fuerzas del orden actúan en nombre de clientes a los que han robado el dispositivo o lo han perdido. También recibe peticiones relacionadas con investigaciones de fraude: solicitan normalmente detalles de los clientes de Apple asociados a dispositivos o conexiones a servicios de Apple.

AUSTRALIA ES QUIEN SOLICITA MÁS DATOS DE CLIENTES ASOCIADOS A DISPOSITIVOS O CONECTADOS A SERVICIOS DE APPLE

Peticiones basadas en dipositivos y % para las que Apple proporcionó datos

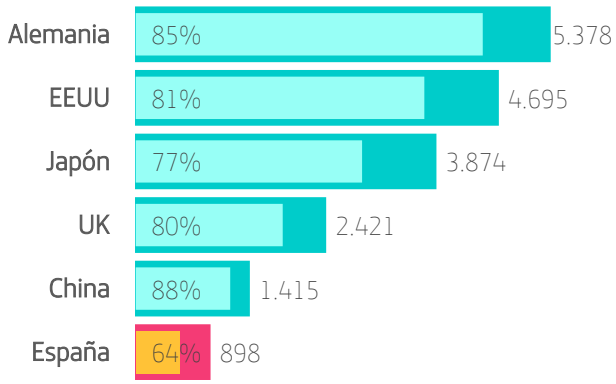


Peticiones basadas en datos financieros

Se producen estas peticiones cuando las fuerzas del orden actúan en nombre de clientes que requieren asistencia relacionada **con actividad fraudulenta de tarjetas de crédito o tarjetas regalo que se han usado para comprar productos de Apple.**

ALEMANIA ES EL PAÍS CON MÁS PETICIONES DE DATOS FINANCIEROS

Peticiones basadas en datos financieros y % para las que Apple proporcionó datos

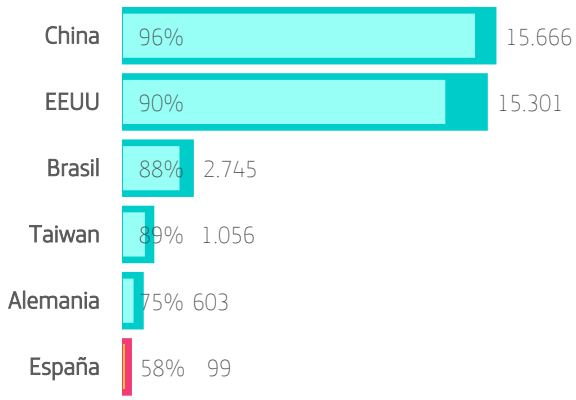


Peticiones basadas en cuentas

Se realizan **peticiones a Apple relacionadas con cuentas que pueden haber sido usadas en contra de la ley y términos de uso de Apple**. Se trata de cuentas de iCloud o iTunes y su nombre, dirección e incluso contenido en la nube (backup, fotos, contactos...).

CHINA Y EEUU SON LOS QUE MÁS SOLICITAN INFORMACIÓN SOBRE CUENTAS DE APPLE

Peticiones basadas en cuentas y % para las que Apple proporcionó datos



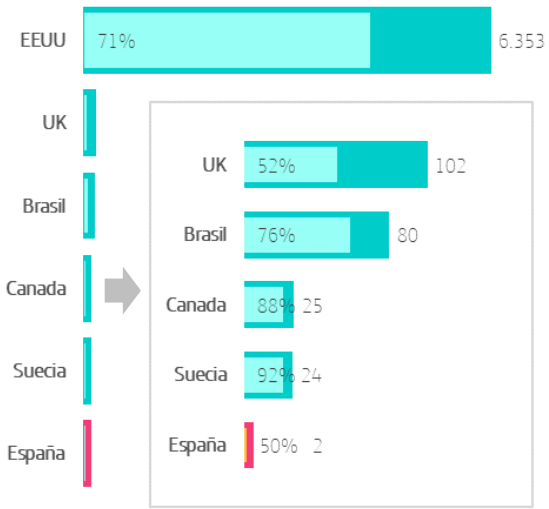
Esta es quizás la medida más intrusiva, en la que Apple proporciona contenido real privado. **China y Estados Unidos son los que más datos solicitan**. Curiosamente, a China se le hace caso hasta en un 96% de las veces, mientras que a Estados Unidos "solo" en un 90%. Apple tiene la potestad de negarse si considera algún fallo en forma o fondo. Hay que tener en cuenta que Apple, además de ofrecer los datos, puede ofrecer "metadatos" no relacionados directamente con los datos, y esto no cuenta como petición "satisfecha" aunque también incluye ofrecer información.

Peticiones relacionadas con la preservación de cuentas

Bajo el contexto de la U.S. Electronic Communications Privacy Act (ECPA), se puede solicitar a Apple que "congele" los datos de una cuenta y los mantenga desde 90 a 180 días. Este es un paso previo a petición de acceso a la cuenta, en espera de que se obtenga el permiso legal para solicitar datos y para evitar que la cuenta sea borrada por el investigado.

EEUU ES EL PAÍS QUE MÁS SOLICITA LA PRESERVACIÓN DE CUENTAS

Peticiones relacionadas con la preservación de cuentas y % para las que Apple las preservó

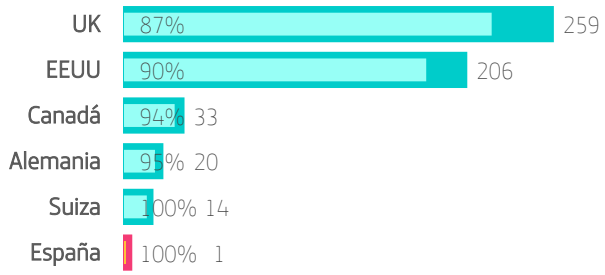


Peticiones por emergencias

También amparados bajo la U.S. Electronic Communications Privacy Act (ECPA), es posible solicitar a Apple que **proporcione datos privados de cuentas si en situaciones de emergencia se cree que esto puede evitar un peligro de muerte o daño serio a individuos.**

UK LIDERA LAS PETICIONES POR EMERGENCIAS

Peticiones por emergencias y % para las que Apple proporcionó datos



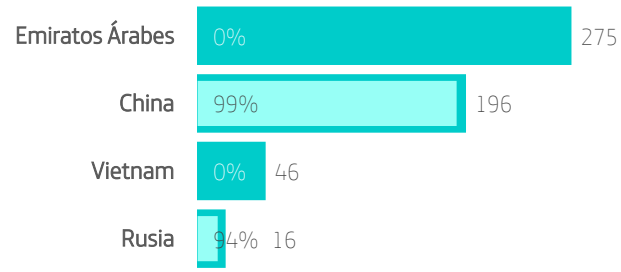
Curiosamente aquí gana el Reino Unido con 259 cuentas pedidas, aunque no siempre se les satisface, seguido muy de cerca por Estados Unidos. El resto de países realizan apenas decenas de peticiones, casi siempre satisfechas. ¿Se preocupa más el Reino Unido por las emergencias y se limita a solicitar datos cuando se da ese caso?

Peticiones relacionadas con la retirada de apps del market

Habitualmente tiene que ver con apps que se supone violan la ley.

GRAN INTERÉS DE EMIRATOS ÁRABES EN ELIMINAR APPS QUE CONSIDERA ILEGALES

Peticiones de eliminación de apps y % para las que Apple proporcionó datos



Emiratos Árabes es, de largo, el país que más retiradas de apps solicita. Seguido de China, Vietnam y Rusia. En esta ocasión, Estados Unidos, muy activo en la solicitud de acceso a datos en general, desaparece por completo.

En el informe también se habla de datos requeridos por terceras partes privadas, bajo una petición legal. Hasta 243 peticiones en las que Apple ha satisfecho 69 accesos a información.

Conclusiones

Podríamos concluir que ciertos gobiernos solicitan «demasiado a menudo» acceso a datos, pero también argumentar que puede ocurrir que la Justicia funcione de manera más ágil en ellos, o que el fraude se base más en estas localizaciones. La interpretación es libre. Lo que sí parecen claras son algunas conclusiones basadas en los datos:

- El interés de Emiratos Árabes en la eliminación de aplicaciones que considera ilegales.
- La implicación del Reino Unido (y Estados Unidos, pero Reino Unido solo aparece en esta categoría) en las situaciones de emergencia.
- El carácter preventivo de Estados Unidos, que solicita congelación de cuenta mucho más a menudo que ningún otro país del mundo.
- Alemania muy implicada (de nuevo, junto a Estados Unidos) en los fraudes financieros relacionados con productos de Apple.
- Australia, Alemania, EEUU y Corea del sur, las naciones que más datos personales solicitan.

Aclaración: en este ejercicio hemos representado en gráficas las tablas que publica la propia Apple. Es importante especificar que todas las peticiones se realizan por lotes. Por ejemplo, Apple contabiliza el número de peticiones de retirada de apps, y a su vez cada petición puede contener un número indeterminado de apps en ellas. Igual con las peticiones de cuentas y el número de cuentas en cada petición. Cuando Apple habla del porcentaje de peticiones satisfechas, habla de eso, de peticiones, pero no de cuentas concretas. Por ejemplo: Apple recibe 10 peticiones, con 100 cuentas entre todas las peticiones y luego dice que ha satisfecho el 90% de las peticiones, no sabemos cuántas cuentas individuales se le han proporcionado. Sin embargo en las gráficas hemos contrastado números totales contra ese porcentaje. Es un ejercicio que si bien no es exacto, puede aportarnos una idea aproximada de la cantidad real de datos proporcionados.

Android

Noticias destacables

Se acabaron los dulces. Google cambia la denominación que hacía referencia a nombres de pasteles y golosinas. Android 9 "Pie" fue el último sistema en tener un sobrenombre derivado de la confitería. A partir de ahora dicho seudónimo se cae y las versiones serán llamadas por su número únicamente.

Ya tenemos a Android 10 desde el 3 de septiembre. Respecto a las novedades que trae el nuevo sistema, destaca en el apartado de la privacidad **la gestión de permisos por aplicación de la geolocalización en segundo plano.** Esta nueva característica permite a un usuario decidir si una aplicación puede obtener datos de posicionamiento si no se está ejecutando en primer plano. Sin duda, una aportación que valorarán positivamente los usuarios más preocupados por su privacidad.

Se añade un método para producir direcciones MAC aleatorias de forma predeterminada. Esto permite o dificulta que no se haga un seguimiento del dispositivo a través de balizas Bluetooth o puntos de acceso WiFi. Aunque se deja un método en la API de desarrollador para que las aplicaciones puedan obtener la dirección hardware real del fabricante.

Respecto al apartado de cifrados y certificados, desde está versión **los certificados firmados con SHA1 dejan de ser confiables**. Esto significa que se rechazarán las conexiones con servidores que posean un certificado firmado con este algoritmo.

Siguiendo con las novedades en el apartado de cifrados, también **se deja de dar soporte a los conjuntos de cifrados de SHA-2 basados en CBC (Counter-Block Chain), considerados menos seguros que su alterativa, GCM.**

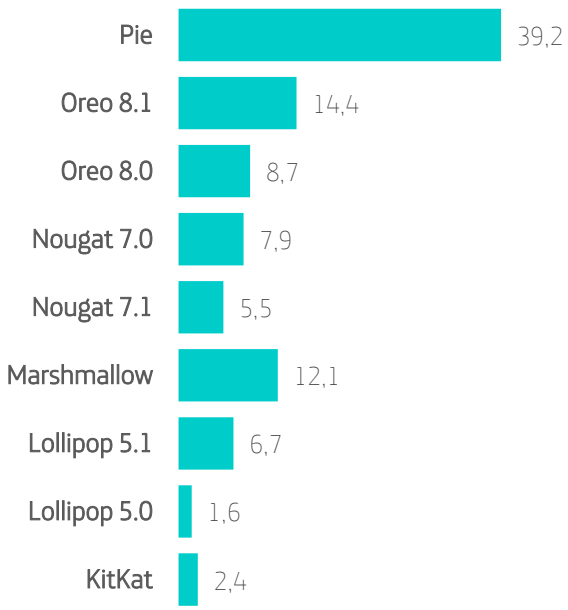
Fragmentación en sistemas Android

La fragmentación sigue siendo la asignatura pendiente para desarrolladores y usuarios en el ecosistema de la plataforma móvil Android. Actualmente, el proyecto Android ya no publica estadísticas en el portal de desarrolladores que muestren el estado de la fragmentación de versiones, por lo que los datos son aquellos disponibles en fuentes públicas. Esto es, no contrastados con fuentes oficiales.

En concreto, no se dispone de datos de la introducción de Android 10; sistema con algo más de tres meses de antigüedad. No obstante, podemos observar como su antecesor, Android 9, aún posee algo más del 22% de cuota, seguido por 8.1, 8.0 y 6.0 con un share alrededor del 15% cada uno. Por debajo del doble dígito se estratifica entre las versiones 7, 5 y 4.

Como podemos apreciar, los terminales Android con mayor antigüedad se niegan a jubilarse. Esto constata que es posible alargar la vida de un terminal más años que el ciclo normal de sustitución. No obstante, la contraprestación es el riesgo que conlleva usar un sistema operativo sin soporte. Esto desde la perspectiva de la seguridad es evidente: nos exponemos a perder el control del dispositivo, así como de sus contenidos. El impacto sobre nuestra privacidad puede ser igualmente crítico.

FRAGMENTACIÓN EN ANDROID
2019-H2



Evolución de vulnerabilidades en Android durante el primer semestre de 2019

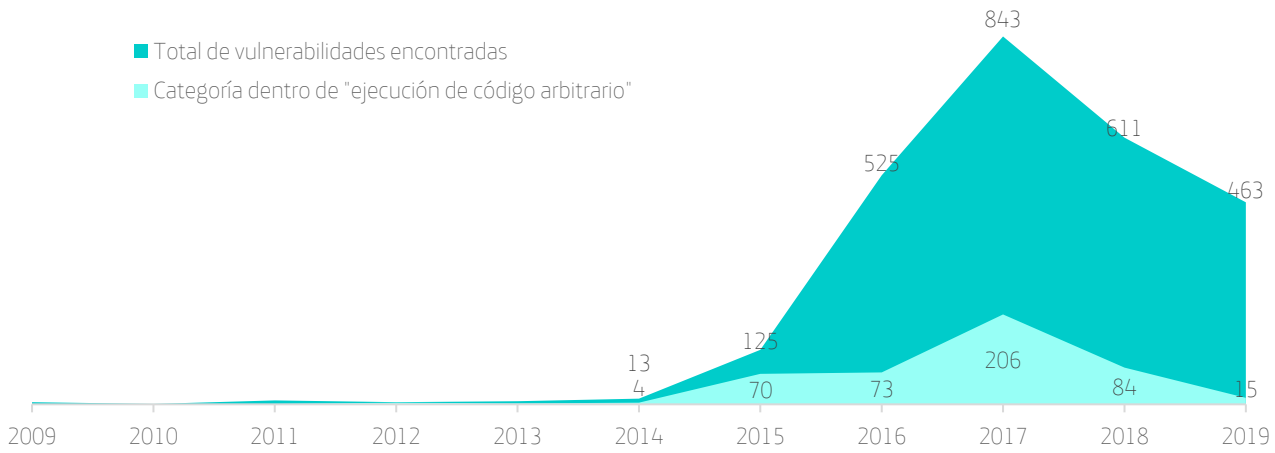
Se han publicado **un total de 463 vulnerabilidades para la plataforma móvil de Google.** Aunque parte de ellas solo afectan a determinadas configuraciones dependientes del fabricante. Por ejemplo, el CVE-2019-14783, solo afecta a teléfonos del fabricante Samsung N(7.x), O(8.x) y P(9.0). Del total de 463 vulnerabilidades, 15 de ellas poseen una puntuación CVSS base igual o superior a 9 junto con la posibilidad de ejecutar código arbitrario.

Una vulnerabilidad de Android cotiza a 2.5 millones de dólares según la compañía Zerodium. Matizar, que este precio se paga si se presenta un exploit con capacidad de comprometer un dispositivo Android "sin" intervención de la víctima. Finalmente, estos precios han de ser tomados con cierta precaución, puesto que las negociaciones entre investigadores y brokers no son públicas y los precios finales rara vez son filtrados.

Los números de vulnerabilidades no dejan lugar a dudas. Android es una plataforma bastante popular para los cazadores de vulnerabilidades. No por ello ha de considerarse insegura, simplemente, posee más tracción o interés por diferentes motivaciones, entre ellas, el programa de recompensas y el mercadeo de exploits.

VULNERABILIDADES EN ANDROID 2019-H2

Evolución de vulnerabilidades por año



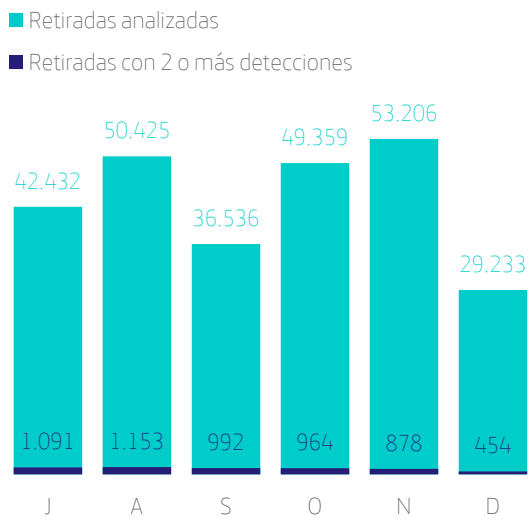
Retirada de apps de Google Play

Este semestre, Google Play ha retirado alrededor de 250.000 apps del market. De ellas, cada mes, entre un 2 y un 3% son detectadas por dos o más motores antivirus de Metadefender de OPSWAT.

La mayor fuente de APK de OPSWAT es su alianza con Telefónica, que envía continuamente nuevos archivos APK e IPA publicados en varios mercados de aplicaciones móviles. El resto de los APK provienen de la comunidad de usuarios de MetaDefender Cloud que envía archivos para escanear, así como de asociaciones de intercambio de malware.

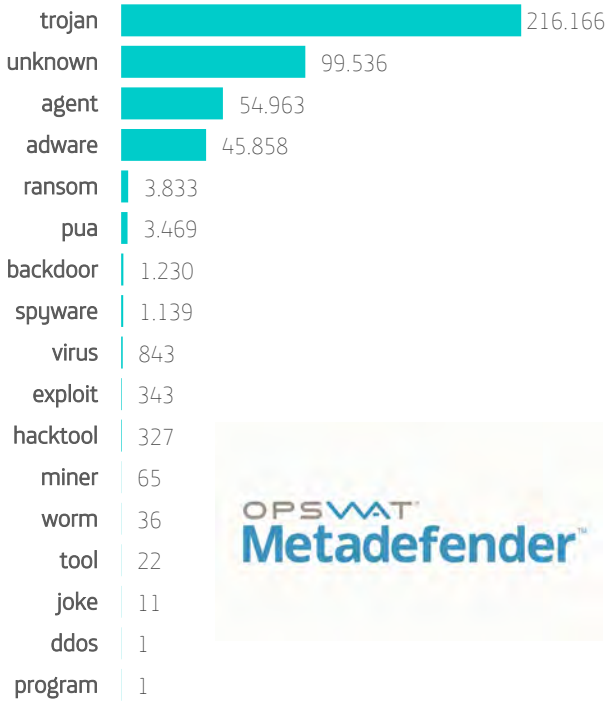
ENTRE UN 2 Y 3% DE LAS APPS RETIRADAS POR GOOGLE PLAY SON DETECTADAS POR DOS O MÁS MOTORES ANTIVIRUS

Número de apps retiradas de Google Play



DENTRO DE LAS CATEGORÍAS MENOS GENÉRICAS, EL ADWARE Y RANSOMWARE PARA ANDROID SON MUY DETECTADOS

Tipos de amenaza en los archivos inyectados (una apk puede estar en varias categorías).



Escaneo de malware en aplicaciones Android

En general, el sistema de OPSWAT ha escaneado 3.607.759 APKs únicos durante el segundo semestre de 2019 y ha encontrado 356.571 de ellos infectados. Los archivos infectados pueden agruparse en los siguientes tipos de amenazas (un apk puede clasificarse en más de un tipo de amenazas):

VULNERABILIDADES DESTACABLES

Comentamos en esta sección algunas de las vulnerabilidades quizás no tan populares pero notables a nuestro juicio de este segundo semestre de 2019. Es decir, aquellas que destacan por su especial relevancia o peligrosidad.

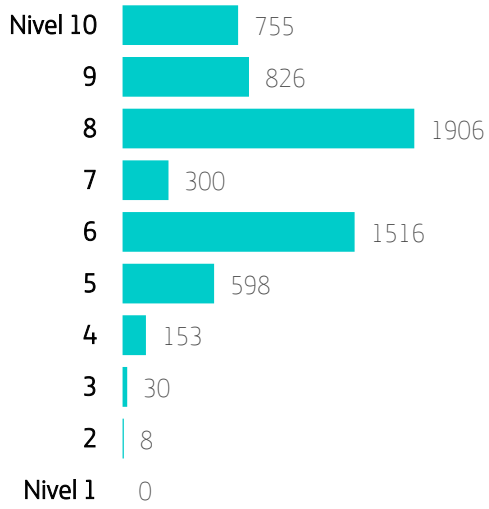
CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING (CVSS V3.0)
CVE-2019-12643	Cisco IOS XE	A finales de agosto se hizo pública una vulnerabilidad en el contenedor de servicios virtuales de la API REST de Cisco para el Software IOS XE de Cisco. Este fallo, podría permitir a un atacante remoto no autenticado evadir la autenticación en un dispositivo IOS XE de Cisco. La vulnerabilidad se debe a una comprobación inadecuada en la gestión del servicio de autenticación de la REST API. Un atacante podría explotar esta vulnerabilidad enviando peticiones HTTP maliciosas al dispositivo afectado. Un exploit exitoso podría permitir al atacante obtener el token-id de un usuario autentificado. Este token-id podría utilizarse para evadir la autenticación y ejecutar acciones privilegiadas a través de la interfaz del contenedor de servicio virtual de la API REST en el dispositivo Cisco IOS XE afectado. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-iosxe-rest-auth-bypass	10.0
CVE-2019-1372	Microsoft Azure Stack	También en agosto, Microsoft publicó un boletín de seguridad que afectaba a su plataforma de computación en nube híbrida: Azure Stack. El fallo se debía al no ser correctamente comprobada la longitud de un búfer antes de copiar memoria en él. Un atacante podría hacer que una función sin privilegios ejecutada por el usuario se adoptase el contexto de la cuenta NT AUTHORITY\system. Esto posibilitaría la evasión de la sandbox. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1372	10.0
CVE-2019-13917 CVE-2019-15846	Servidor de correo Exim	Mal semestre para Exim. Comenzó septiembre con dos graves vulnerabilidades que prácticamente ponían en bandeja al sistema debido a que, una explotación exitosa, permitía la ejecución de código arbitrario con permisos de root. Una de ellas era debido al operador de expansión “sort”, la otra debido a un desbordamiento de memoria intermedia que ocurría durante la negociación TLS con el servidor Exim. En ninguno de los dos casos era necesario poseer usuario en el servidor por lo que el fallo era especialmente crítico para uno de los servidores de correo “open source” con más instalaciones.	10.0

Las vulnerabilidades en cifras

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

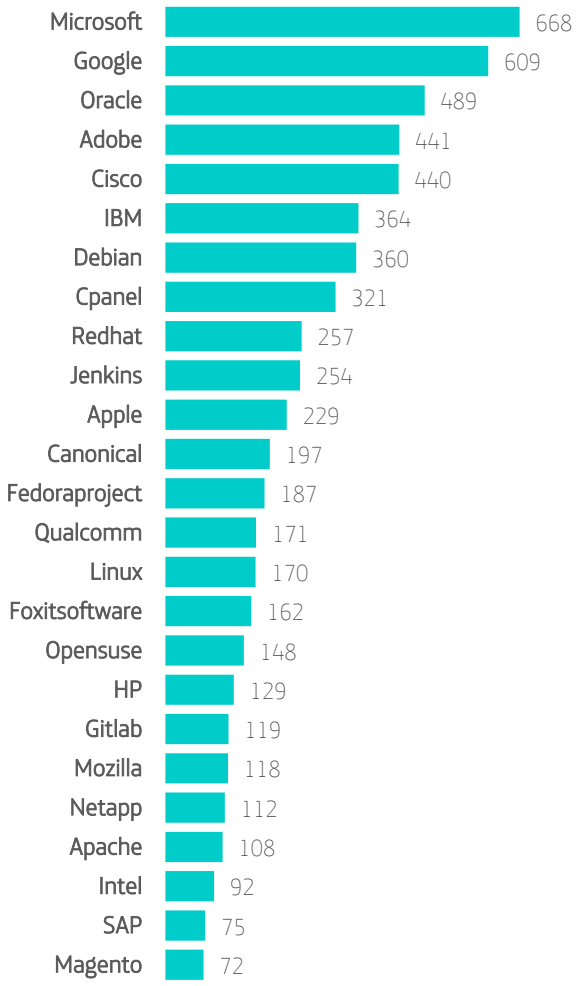


Top 25 compañías con más CVE acumulados

Como en otras ocasiones, hemos de relativizar los datos aquí expuestos. Esto es debido a que algunos fabricantes poseen numerosos productos candidatos a obtener un CVE, como puede ser el caso de Oracle y su cuantioso catálogo de productos (alta dispersión). Por el contrario, compañías con un número menor de productos candidatos, sí poseen una gran concentración de CVE en ciertos productos (alta concentración), como puede ser Adobe con Flash y Reader, que acumulan un alto número de vulnerabilidades.

VULNERABILIDADES

Top 25 fabricantes por CVE acumulados



Debemos hacer notar también que existen vulnerabilidades con transversalidad. Es decir, Canonical (que es sinónimo de Ubuntu), Debian, FedoraProject, openSUSE y ReadHat comparten un gran número de binarios y bibliotecas, además del mismo núcleo del sistema operativo: el kernel Linux. Cuando en realidad se trata de una misma vulnerabilidad o CVE, su parche se distribuye a todos los fabricantes, quienes elaboran un paquete para su o sus distribuciones particulares.

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.

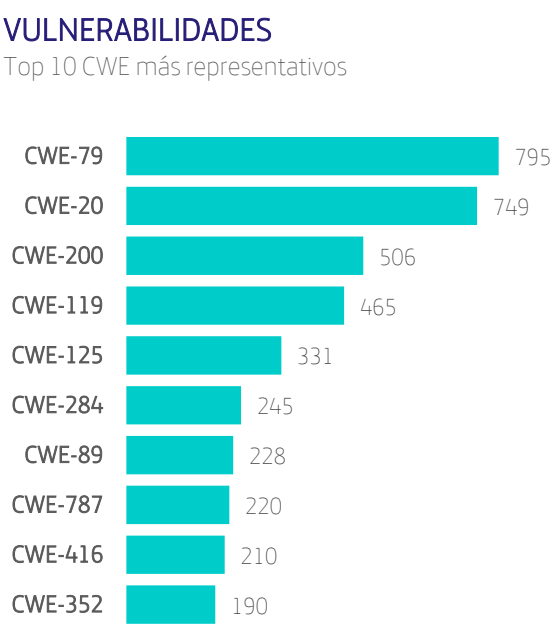


Tabla descriptiva de cada CWE

CWE	TÍTULO	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.	795
CWE-20	Improper Input Validation	Categoría general para errores que consisten en un control deficiente o inexistente en entradas de datos procedentes de usuario.	749
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.	506
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.	465
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.	331
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 recoge 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.	245
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).	238
CWE-89	Improper Neutralization of Special Elements used in a SQL Command (SQL Injection)	Básicamente, recoge la inyección de código SQL en una cadena de consulta a través de parámetros o entrada de datos a la aplicación.	228

CWE-787	Out-of-Bounds Write	Relacionada con CWE-125, agrupa aquellas vulnerabilidades que permiten escribir más allá de los límites designados a una región reservada de memoria intermedia.	220
CWE-416	Use After Free	Fallo en la gestión de memoria de un proceso que permite llamar a un objeto o referenciar una zona de memoria en el montículo que ha sido liberada previamente.	210
CWE-352	Cross-site Request Forgery (CSRF)	Se trata de aquellas vulnerabilidades (generalmente, en entorno web) que causan una ausencia o defecto en la validación de peticiones correctas desde un cliente. Es decir, una aplicación no puede o sabe distinguir si la petición ha llegado desde una acción legítima y consciente de un usuario, o se trata de una petición maliciosamente creada y disparada por un usuario desde un sitio controlado por un atacante.	190

Conclusiones

Nuevamente, y no es sorpresa, se cuelan vulnerabilidades que muestran una falta de control sobre los límites de escritura o lectura de buffers, mala gestión en la liberación de memoria o falta de filtrado en las peticiones o parámetros procedente de usuario.

Las vulnerabilidades siguen ascendiendo en número. El mercado de exploits sigue cotizando al alza. Con este panorama, es difícil contemplar un escenario distinto. **La industrialización en la búsqueda de fallos de seguridad en sistemas y aplicaciones ha creado un ecosistema perfecto para el descubrimiento de nuevos vectores y nuevas herramientas**.

A pesar incluso de la adopción de nuevos lenguajes (Go, Rust...) que permiten obtener una gestión más adecuada de la memoria, mejor *tooling* y nuevas librerías que le conceden un papel protagonista a la seguridad, todavía es pronto para notar una mejora perceptible en este aspecto. Un efecto que tardará, sin duda, mucho más tiempo del deseado; e incluso así, se descubrirán nuevos caminos y vías para comprometer un sistema que no se hayan concebido antes.

QUIÉN ES QUIÉN DESCUBRIENDO VULNERABILIDADES MICROSOFT

¿Quién encuentra más vulnerabilidades en los productos de Microsoft? **¿Qué porcentaje de vulnerabilidades son descubiertas por la propia Microsoft, empresas o brókeres de vulnerabilidades? ¿Cuántos fallos no se sabe quién los ha descubierto?** En este informe hemos analizado lo datos de los últimos tres años y medio para entender quién resuelve qué en el mundo de los productos Microsoft y la gravedad de estos fallos. Asimismo, **nos permite disponer de una visión interesante sobre quién investiga realmente los productos de Microsoft, los reporta de manera responsable, así como cuántas vulnerabilidades están acreditadas y cuántas no** (lo que podría suponer que son descubiertas por atacantes).

Cada segundo martes del mes Microsoft publica sus tradicionales parches de seguridad en un único paquete que actualiza Windows. Esa actualización resuelve una serie de CVEs o vulnerabilidades. Pero no siempre fue así. Durante muchos años se publicaron boletines que ocultaron varios CVEs, normalmente agrupados por producto.

Desde hace muchos años Microsoft viene incorporando en su política de desarrollo seguro la auditoría de su propio código con el objetivo de mejorar su seguridad. Hemos querido saber exactamente cuántos fallos de seguridad encuentra la propia compañía en sus auditorías internas, para **así hacernos una idea no solo de cuánto contribuye la propia Microsoft a la mejora de la seguridad de sus productos, sino de cuánto contribuyen también el resto de habituales *bug hunters* de la industria.**

Metodología

Hemos realizado algo muy simple. Hemos recopilado y procesado toda la información de CVEs acreditadas durante el segundo semestre de 2019. La fuente de información ha sido principalmente esta página:

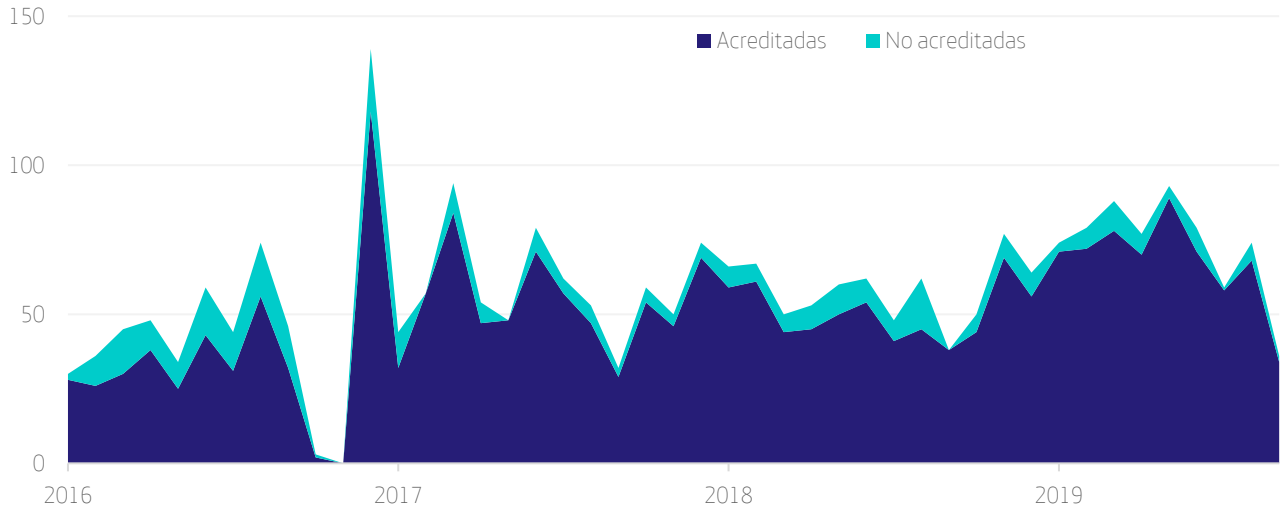
https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments

Estas son las vulnerabilidades acreditadas, esto es, reportadas por alguien identificable, ya sea particular o empresa. En este período hemos analizado 390 vulnerabilidades acreditadas. De todas ellas hemos extraído su gravedad a través del CVSS oficial del NIST.

Este número no suponen el total de fallos descubiertos. En realidad, hemos contado además los fallos no acreditados directamente. Entendemos que la mayoría de estos fallos pueden venir de vulnerabilidades encontradas en 0-days u otras circunstancias en las que no se conoce al autor y no ha sido reportada de forma anónima. En estos casos, Microsoft no acredita a nadie en particular. Esta diferencia entre vulnerabilidades acreditadas y "no acreditadas", que no es lo mismo que anónimas, se ve reflejada en el siguiente gráfico.

NO TODAS LAS VULNERABILIDADES PROCEDEN DE FUENTES ACREDITADAS

Número de Vulnerabilidades Acreditadas y No-Acreditadas desde 2016 a 2019.



De los créditos, hemos extraído la compañía que ha descubierto la vulnerabilidad. **En el caso de que sean varios los descubridores, hemos contado solo al que aparecía en primer lugar, para simplificar los cálculos** y porque entendemos que se muestra como principal analista el que las reportó en primer lugar. Si bien esto puede ser inexacto, da como resultado la fórmula más sencilla. Además, hemos contado dos fallos encontrados por el equipo de Hiper-V como descubiertas por Microsoft.

A partir de ahí, hemos realizado diferentes cálculos para poder analizar quién contribuye más y mejor a mejorar la seguridad de los productos Microsoft, de manera responsable.

Los datos

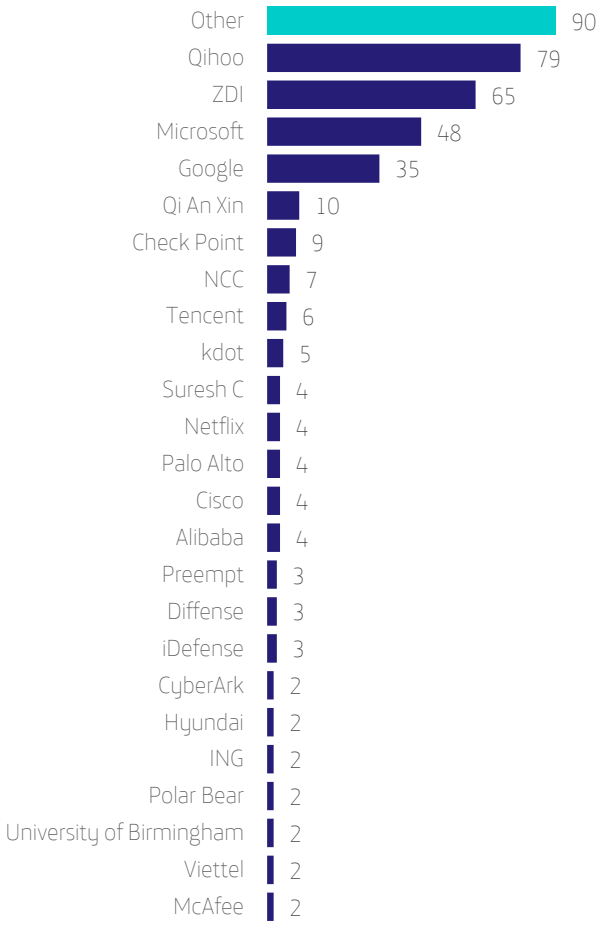
Qihoo es la compañía que más vulnerabilidades ha descubierto en productos de Microsoft en 2019-H2

Qihoo es sin duda la compañía que más colabora en el reporte de vulnerabilidades en productos Microsoft con algo más de un 20% de todos los fallos. Aproximadamente un 23% de los fallos encontrados en productos de Microsoft son reportados por la categoría "otros", que engloba pequeñas empresas que no suelen reportar, o analistas independientes. **El tercer puesto es para la propia Microsoft con algo más del 12% de sus propios fallos. Google viene detrás, con un 9% de los fallos.**

Mención especial merece **Zero Day Initiative de Trend Micro, una iniciativa privada que actúa como "bróker" de vulnerabilidades.** Los investigadores pueden suscribirse a este programa y serán pagados por los fallos encontrados a cambio de cederlos a ZDI, que los reportará de forma responsable a los fabricantes. Esta iniciativa es la fórmula más popular con un 16% de vulnerabilidades reportadas a Microsoft, en segunda posición detrás de Qihoo.

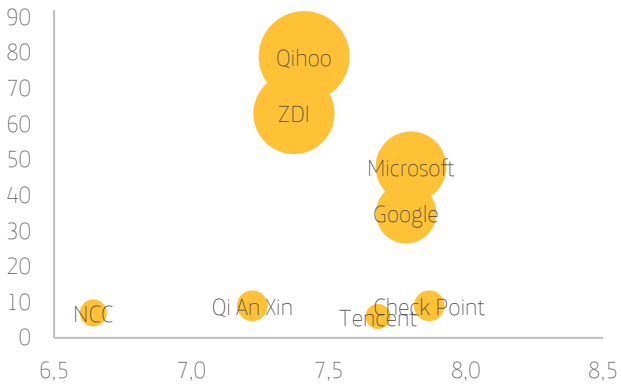
QIHOO ES LA COMPAÑÍA QUE MÁS VULNERABILIDADES DESCUBRE EN PRODUCTOS DE MICROSOFT

Reparto entre los descubridores de las 397 vulnerabilidades en 2019-H2.



QIHOO Y ZDI REPORTAN MÁS VULNERABILIDADES, PERO DE MENOR GRAVEDAD

Distribución de vulnerabilidades por puntuación y por descubridor; el tamaño de la burbuja es proporcional al número de vulnerabilidades descubiertas durante 2019 H2.



Qihoo y ZDI reportan más vulnerabilidades, pero de menor gravedad

Si relacionamos ambos valores (gravedad y número), observamos que, **si bien Qihoo encuentra indiscutiblemente más que cualquier otro fabricante, se mueve en un rango de gravedad menor que el de Microsoft**. Los que reporta Google, que encuentra casi el mismo número que fallos que la propia Microsoft, suelen ser de similar gravedad.

Conclusiones

Durante el segundo semestre de 2019, Qihoo y ZDI han liderado el descubrimiento de vulnerabilidades en productos de Microsoft, con un 20% y 16% del total de vulnerabilidades reportadas por ellos dos, respectivamente. Aproximadamente un 23% de los fallos son reportados por la categoría "otros" que engloba pequeñas empresas que no suelen reportar a menudo, o analistas independientes. El tercer puesto es para la propia Microsoft que descubre algo más del 12% de sus propios fallos. Un 7% de las vulnerabilidades no se atribuyeron a nadie en particular.

Podemos concluir que la mayoría de vulnerabilidades encontradas en Microsoft, de gravedad en torno al 7, son encontradas por cuatro principales actores: Qihoo, ZDI (que aglutina a investigadores independientes), la propia Microsoft y Google. También llama la atención el importante descenso de vulnerabilidades no acreditadas (encontradas de forma no responsable). De un 25% en 2016 a apenas un 9% en 2019, lo que implica una mejor gestión de los fallos, precisamente a través de plataformas como ZDI, donde se compensa a los investigadores y se les motiva a que los fallos se reporten de forma responsable.

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.

Advertimos que la atribución de este tipo de operaciones, así como la composición, origen e ideología de los grupos organizados, es compleja y, necesariamente, no puede ser completamente fiable.

Esto es debido a la capacidad de anonimato y engaño inherente a este tipo de operaciones, en la que los actores pueden utilizar medios para manipular la información de modo que oculte su verdadero origen e intenciones; incluso es posible que en determinados casos actúen con el modus operandi de otros grupos para desviar la atención o perjudicar a estos últimos.

Actividad APT notable, detectada durante el segundo semestre de 2019

Winnti

Aunque lleva operando desde 2010, el grupo chino Winnti ha tenido por objetivos, de forma típica, desarrolladoras de software en general y de videojuegos en particular. Se les supone apoyo institucional del gobierno chino, aunque no se descarta que paralelamente posean una finalidad económica.

El grupo, ha sido objeto de seguimiento y análisis por parte de un grupo de investigadores de ESET, quienes han publicado un extenso trabajo de investigación acerca de las operaciones del citado grupo. A destacar, el uso de técnicas de ocultación una vez han penetrado en una organización, tales como el uso de un servidor Microsoft SQL usado como puerta trasera.

FIN7 o Carbanak

Sobre este grupo ya hemos hablado anteriormente. FIN7 o también conocido como Carbanak, sobre todo cuando saltó la noticia en medios generalistas de la detención de su supuesto líder en España.

Durante este semestre, investigadores de la compañía FireEye, han detectado el uso de dos nuevas técnicas empleadas por el comentado grupo: BOOSTWRITE, un *dropper* con capacidad para descifrar *payloads* incrustados sin necesidad de tocar disco mediante la descarga de una clave de cifrado desde un servidor de control.

El otro nuevo componente, RDFSNIFFER, es un módulo para BOOSTWRITE, específicamente diseñado para atacar al proceso RDFClient del Aloha Control Center Client. Este software es usado en terminales de pago de la compañía NCR Group. Como vemos, es un grupo que sigue centrado en atacar especialmente al sector finanzas.

En conjunto son técnicas nuevas, pero de base conocida: volar por debajo de la línea de radar de los antivirus. Evitar la detección y prolongar la vida útil de cada infección para maximizar los beneficios que pueda reportar un ataque.

APT41

Otro de los grandes actores del momento. APT41 estrecha lazos con grupos tales como el anteriormente citado Winnti o BARIUM. Sobre todo, por el modus operandi y el empleo de ciertas técnicas y herramientas comunes. De hecho, muchos de los objetivos de APT41 coinciden con Winnti, tales como desarrolladoras de videojuegos.

FireEye ha seguido los pasos de las operaciones de este grupo trazando un histórico en un detallado informe. En él, describen las técnicas empleadas y el aprovechamiento de los recursos que extraen de sus víctimas como, por ejemplo, el robo de certificados válidos para la firma de malware; una vía que simplifica la instalación de implantes en los sistemas operativos de los objetivos del grupo.

Este conjunto de técnicas: aprovechar los recursos de una desarrolladora o productora de software, etc., se conoce como "*supply chain compromise*". Agrupa ataques y explotación de recursos de las víctimas que permiten o facilitan la tarea de difundir e instalar el malware bajo control de este tipo de grupos organizados.

A APT41 se le atribuye un origen chino y destaca además por la gran cantidad de malware producido. Se han identificado hasta 46 tipos de familias diferentes y casi 150 herramientas del tipo puerta trasera, keylogger o rootkits.

Lazarus

El nombre de este grupo está ligado a una operación mediáticamente conocida como "el hackeo a Sony Pictures". El grupo, atribuido a Corea del Norte y activo desde 2009, ha sido señalado como el responsable de un ataque a una central nuclear India.

Los hechos fueron notificados por los responsables técnicos de la central al CERT indio el 4 de septiembre. En concreto, la detección de un malware en el área administrativa de la central nuclear de Kudankulam (KKNPP). Es decir, no detectado en las redes de los sistemas de control de la central.

El malware detectado, denominado DTrack y analizado a fondo por la compañía rusa Kaspersky, se encargaría de recabar información de los equipos infectados, así como del tráfico de red y registro de pulsaciones de los teclados (*keylogging*).

El ataque puede ser considerado un acercamiento con objetivo de vigilar y profundizar en la producción de energía (recurso estratégico). A pesar de que las redes de control están aisladas respecto del resto de redes, la red administrativa posee información acerca de fechas de mantenimiento, mensajes, datos, etc. Información vital para la preparación de ataques más planificados sobre las redes de control.

EVALUACIÓN DEL CIBERRIESGO POR SECTORES

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

BITSIGHT®
The Standard in SECURITY RATINGS

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.

Datos de infecciones detectadas y neutralizadas (por sector económico)

A continuación se muestran las cifras agrupadas por sector económico de la media de días efectivos desde que la amenaza es detectada hasta que es neutralizada por la organización, tanto para Europa como para España.

Recopilada a partir de multitud de fuentes variadas:

- Botnet
- Spam
- Código malicioso
- Configuraciones
- DDOS
- Conductas de usuario
- Feeds de noticias
- Social Media

Normaliza y mapea la entrada:

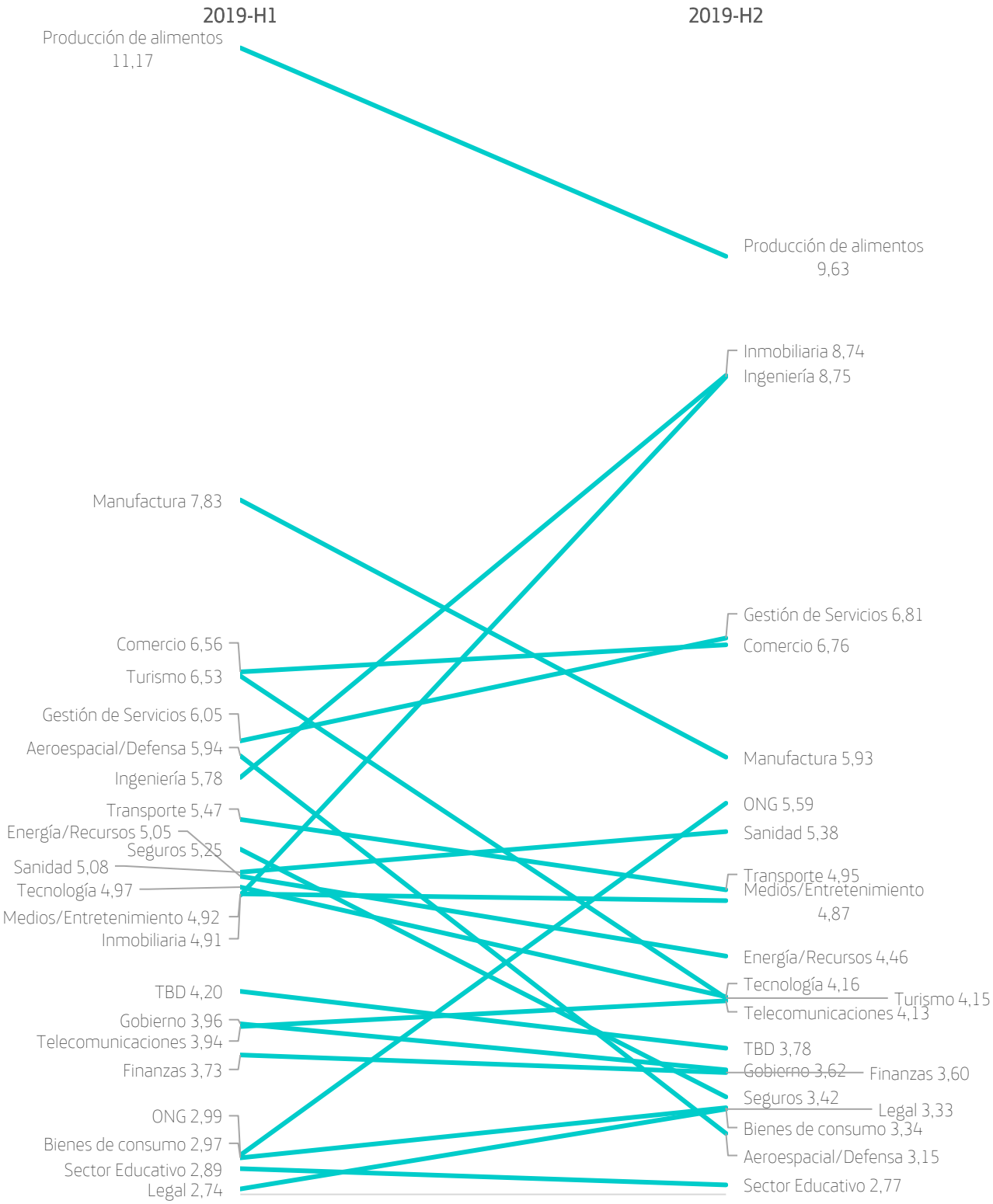
- Tipo de sistema comprometido
- Fecha
- IP de la organización
- Gravedad
- Frecuencia
- Duración
- Confianza

El portal del cliente resume el riesgo de seguridad:

Analítica Ratings Alertas

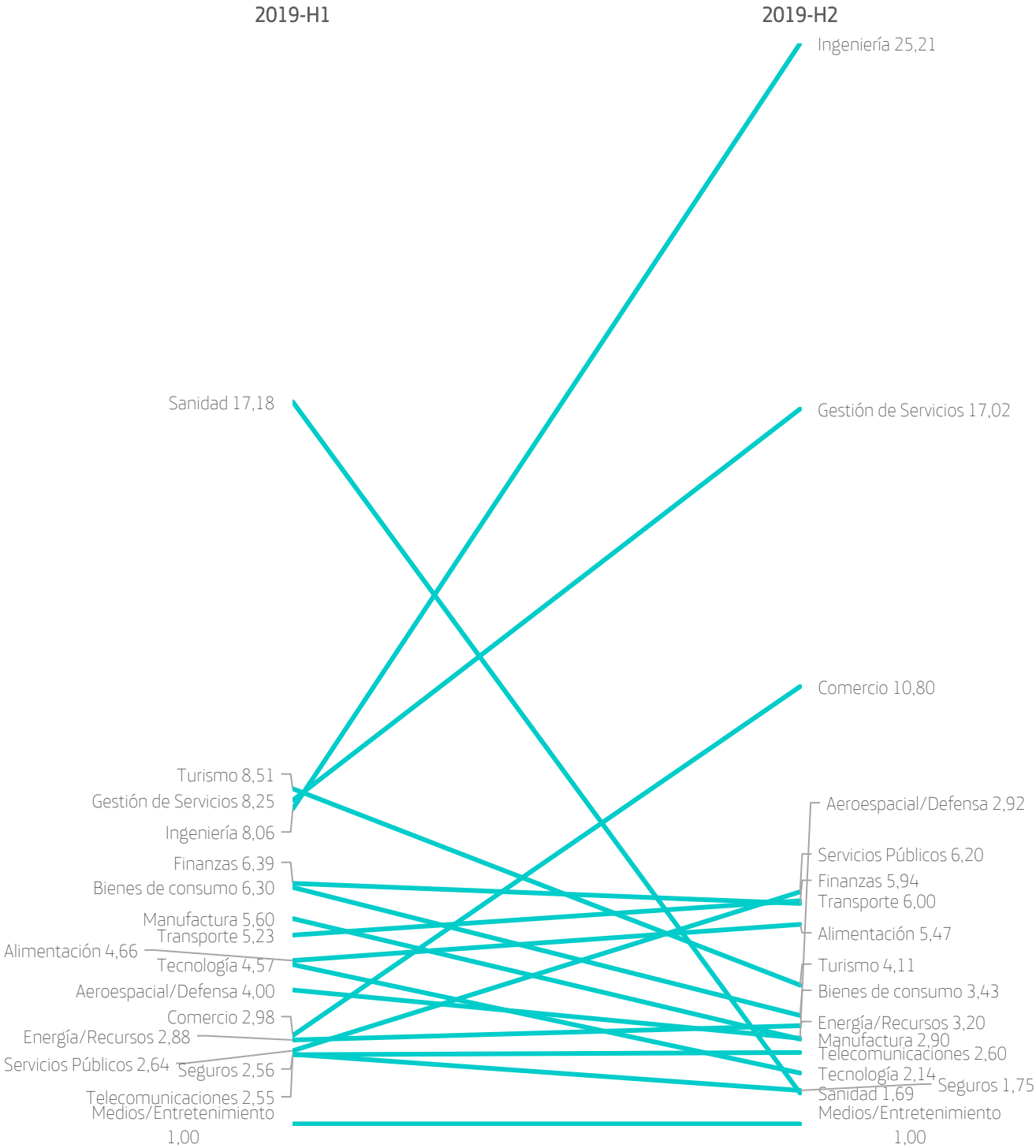
PRÁCTICAS DE SEGURIDAD EN EUROPA

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



PRÁCTICAS DE SEGURIDAD EN ESPAÑA

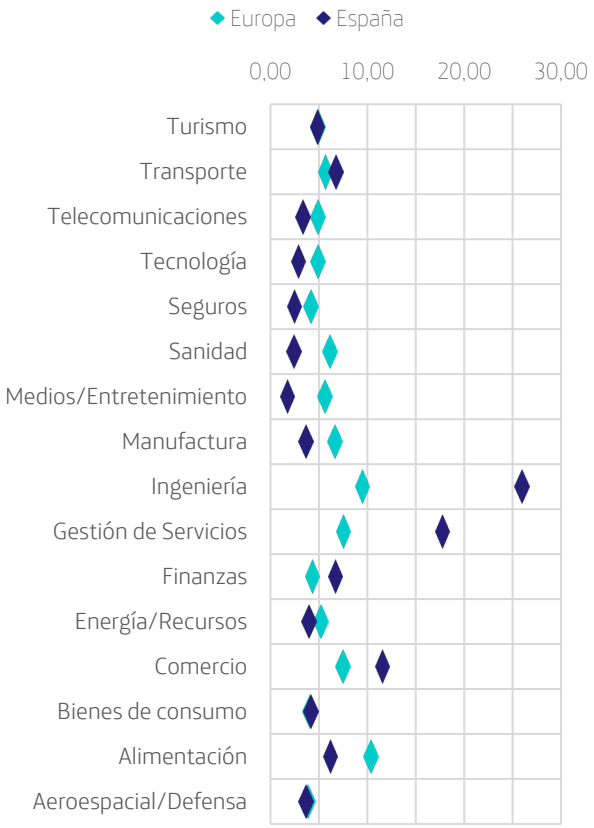
Número medio de **días** efectivos que necesita una **compañía española** para solucionar una amenaza de malware, agrupado por sector



El siguiente gráfico compara el tiempo de respuesta entre España y Europa, durante el segundo semestre de 2019, agrupado por sector.

COMPARATIVA DETECCIÓN-NEUTRALIZACIÓN ENTRE ESPAÑA Y EUROPA DURANTE 2019-H2 POR SECTOR

Medida en número medio de días



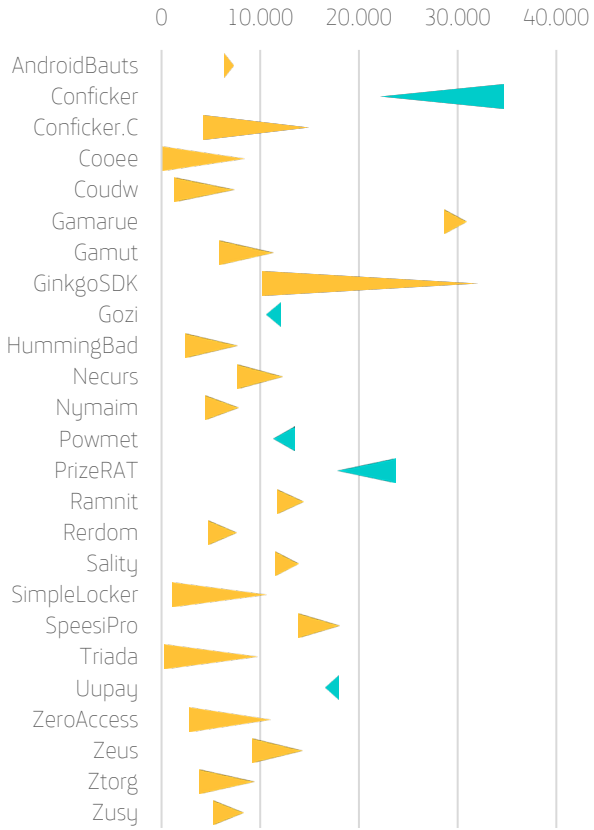
Esto quiere decir, que por ejemplo en el sector de ingeniería se tardan de media unos 9 días en Europa en neutralizar una amenaza, mientras que en España se emplean unos 25.

Las 25 familias de malware e infecciones detectadas en Europa

A continuación, se muestran las 25 familias de malware que más sistemas infectan en Europa, así como el crecimiento experimentado con respecto al ranking anterior.

EVOLUCIÓN DE LAS 25 FAMILIAS DE MALWARE MÁS VIRULENTAS EN EUROPA

Crecimiento (en naranja) o decrecimiento (en azul) experimentado desde 2019-H1 a 2019-H2 medido en sistemas infectados.

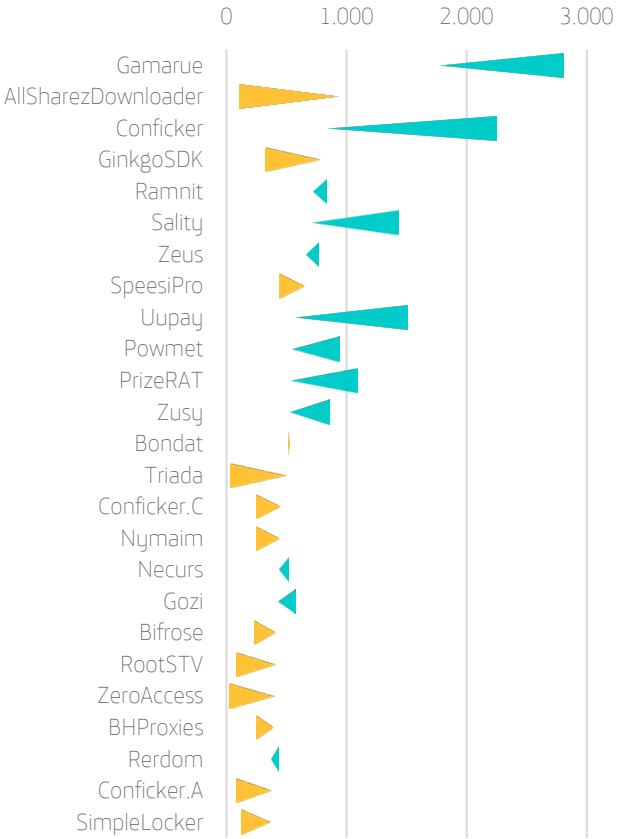


Las 25 familias de malware e infecciones detectadas en España

A continuación, se muestran las 25 familias de malware que más sistemas infectan en España, así como el crecimiento experimentado con respecto al ranking anterior.

EVOLUCIÓN DE LAS 25 FAMILIAS DE MALWARE MÁS VIRULENTAS EN ESPAÑA

Crecimiento (en naranja) o decrecimiento (en azul) experimentado desde 2019-H1 a 2019-H2 medido en sistemas infectados.



RECAPITULACIÓN

Durante este semestre, **se han parcheado 198 CVE en en IOS.** 13 poseen la categoría de críticos y 6 de ellos permiten la ejecución de código arbitrario. Las cifras representan un aumento respecto del semestre anterior, superando así los periodos anteriores.

Australia es el país que solicita más datos de clientes asociados a dispositivos o conectados a servicios de Apple, Alemania el que más datos financieros, China y EEUU los que más solicitan sobre información de cuentas. **Los Emiratos Árabes han solicitado eliminar 275 apps pero ninguna petición les ha sido concedida.**

Se han publicado **un total de 463 vulnerabilidades para Android.** 15 de ellas poseen una puntuación CVSS base igual o superior a 9 junto con la posibilidad de ejecutar código arbitrario.

Este semestre, Google Play ha retirado alrededor de 250.000 apps del market. De ellas, cada mes, entre un 2 y un 3% son detectadas por dos o más motores antivirus

Durante el segundo semestre de 2019, Qihoo y ZDI han liderado el descubrimiento de vulnerabilidades en productos de Microsoft, con un 20% y 16% del total de vulnerabilidades reportadas por ellos dos, respectivamente. Aproximadamente un 23% de los fallos son reportados por la categoría "otros" que engloba pequeñas empresas que no suelen reportar a menudo, o analistas independientes. El tercer puesto es para la propia Microsoft que descubre algo más del 12% de sus propios fallos. Un 7% de las vulnerabilidades no se atribuyeron a nadie en particular.

Conficker desciende, pero sigue siendo una de las amenazas más destacadas detectada según BitSight en todos los sectores. El sector "gestión de servicios" y comercio son los que más tardan en solucionar una infección en España.

Acerca de ElevenPaths

En ElevenPaths, la unidad global de ciberseguridad del Grupo Telefónica, creemos que es posible un mundo digital más seguro. Apoyamos a nuestros clientes en su **transformación digital,** creando **innovación disruptiva**, aportando la privacidad y la confianza necesaria en nuestra vida digital diaria.

Combinamos la frescura y energía de una start-up con la potencia, conocimiento y robustez de Telefónica, contribuyendo con soluciones que posibilitan la prevención, detección y respuesta ante amenazas diarias en nuestro mundo digital.

Generamos alianzas estratégicas que permiten ampliar la seguridad de nuestros clientes y además, colaboramos con organismos y entidades como la Comisión Europea, CyberThreat Alliance, ECSO, EuroPol, Incibe, y la Organización de los Estados Americanos (OEA).