elevenpaths.com

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.

El primer semestre de 2020 se ha visto marcado en el ámbito de la ciberseguridad por el mismo evento que ha sacudido al mundo entero: la aparición y efectos causados por el SARS-CoV-2. A nadie se les escapa que el éxito de aplicaciones de vídeo conferencia como ZOOM (y el consiguiente descubrimiento de varias vulnerabilidades) ha sido en gran parte motivado por su uso masivo a medida que la pandemia avanzaba por el mundo y se restringían viajes y reuniones. **El asunto ha tenido el impacto suficiente como para ser utilizado como anzuelo en ataques de phishing, dirigido o no, para lograr engañar al receptor, ávido de información en momentos complicados.**

Sin embargo, no todo ha sido el SARS-CoV-2. En el ámbito móvil, Apple presentó iOS 14, dejando atrás así un sistema operativo que no ha representado una buena versión desde el punto de vista de la seguridad.

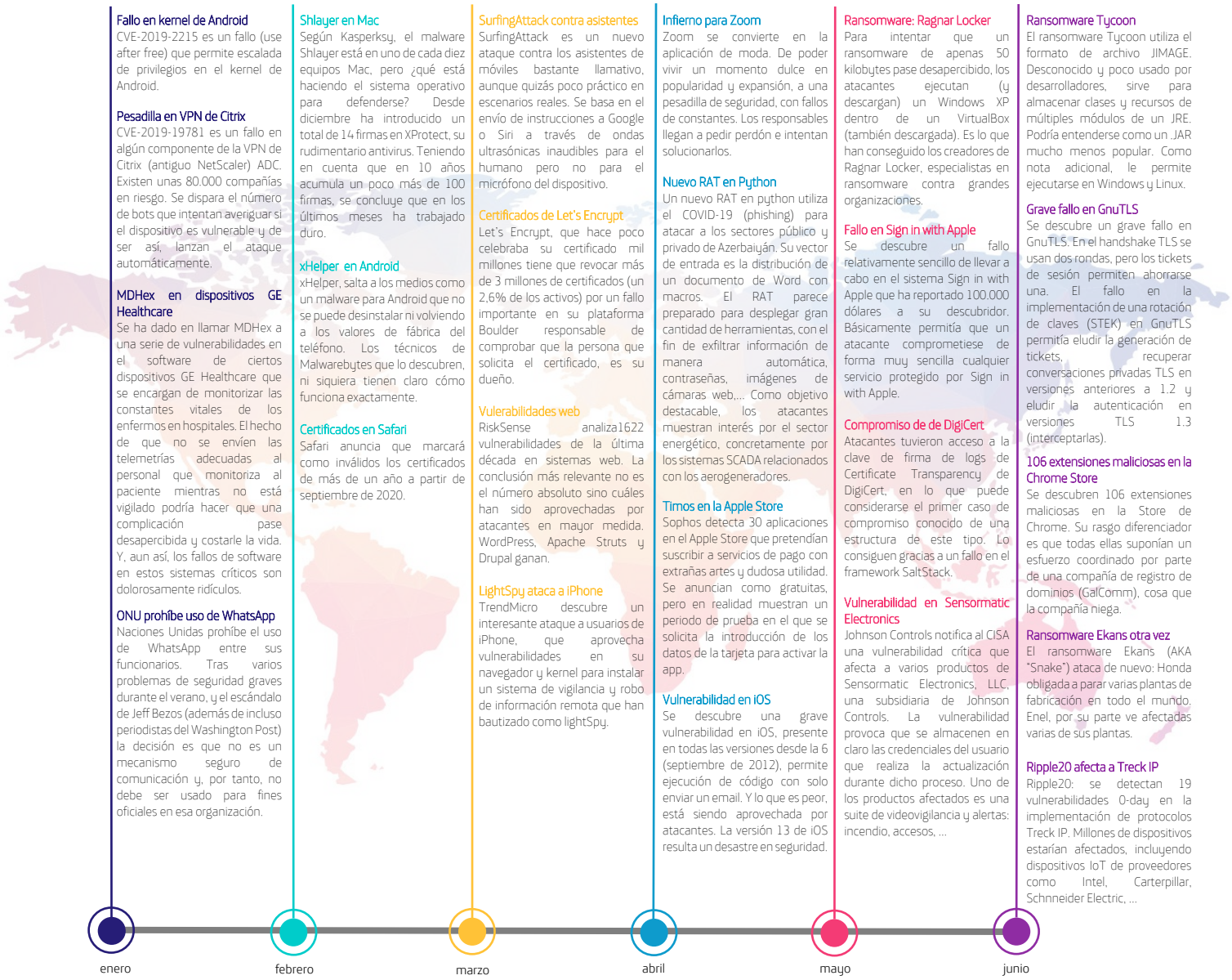
Por su parte, **Google anunció en enero su libro blanco de Android, donde expone las mejoras y características de seguridad de la plataforma móvil de Google.**

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.

¡Allá vamos!

LOS INCIDENTES MÁS DESTACADOS DEL PRIMER SEMESTRE DE 2020

A continuación, damos cuenta de aquellas noticias que mayor impacto han tenido durante el transcurso de este primer semestre de 2020.



Fallo en kernel de Android

CVE-2019-2215 es un fallo (use after free) que permite escalada de privilegios en el kernel de Android.

Pesadilla en VPN de Citrix

CVE-2019-19781 es un fallo en algún componente de la VPN de Citrix (antiguo NetScaler) ADC. Existen unas 80.000 compañías en riesgo. Se dispara el número de bots que intentan averiguar si el dispositivo es vulnerable y de ser así, lanzan el ataque automáticamente.

MDHex en dispositivos GE Healthcare

Se ha dado en llamar MDHex a una serie de vulnerabilidades en el software de ciertos dispositivos GE Healthcare que se encargan de monitorizar las constantes vitales de los enfermos en hospitales. El hecho de que no se envíen las telemetrías adecuadas al personal que monitoriza al paciente mientras no está vigilado podría hacer que una complicación pase desapercibida y costarle la vida. Y, aun así, los fallos de software en estos sistemas críticos son dolorosamente ridículos.

ONU prohíbe uso de WhatsApp

Naciones Unidas prohíbe el uso de WhatsApp entre sus funcionarios. Tras varios problemas de seguridad graves durante el verano, y el escándalo de Jeff Bezos (además de incluso periodistas del Washington Post) la decisión es que no es un mecanismo seguro de comunicación y, por tanto, no debe ser usado para fines oficiales en esa organización.

Shlayer en Mac

Según Kasperksy, el malware Shlayer está en uno de cada diez equipos Mac, pero ¿qué está haciendo el sistema operativo para defenderse? Desde diciembre ha introducido un total de 14 firmas en XProtect, su rudimentario antivirus. Teniendo en cuenta que en 10 años acumula un poco más de 100 firmas, se concluye que en los últimos meses ha trabajado duro.

xHelper en Android

xHelper, salta a los medios como un malware para Android que no se puede desinstalar ni volviendo a los valores de fábrica del teléfono. Los técnicos de Malwarebytes que lo descubren, ni siquiera tienen claro cómo funciona exactamente.

Certificados en Safari

Safari anuncia que marcará como inválidos los certificados de más de un año a partir de septiembre de 2020.

SurfingAttack contra asistentes

SurfingAttack es un nuevo ataque contra los asistentes de móviles bastante llamativo, aunque quizás poco práctico en escenarios reales. Se basa en el envío de instrucciones a Google o Siri a través de ondas ultrasónicas inaudibles para el humano pero no para el micrófono del dispositivo.

Certificados de Let's Encrypt

Let's Encrypt, que hace poco celebraba su certificado mil millones tiene que revocar más de 3 millones de certificados (un 2,6% de los activos) por un fallo importante en su plataforma Boulder responsable de comprobar que la persona que solicita el certificado, es su dueño.

Vulerabilidades web

RiskSense analiza1622 vulnerabilidades de la última década en sistemas web. La conclusión más relevante no es el número absoluto sino cuáles han sido aprovechadas por atacantes en mayor medida. WordPress, Apache Struts y Drupal ganan.

LightSpy ataca a iPhone

TrendMicro descubre un interesante ataque a usuarios de iPhone, que aprovecha vulnerabilidades en su navegador y kernel para instalar un sistema de vigilancia y robo de información remota que han bautizado como lightSpy.

Infierno para Zoom

Zoom se convierte en la aplicación de moda. De poder vivir un momento dulce en popularidad y expansión, a una pesadilla de seguridad, con fallos de constantes. Los responsables llegan a pedir perdón e intentan solucionarlos.

Nuevo RAT en Python

Un nuevo RAT en python utiliza el COVID-19 (phishing) para atacar a los sectores público y privado de Azerbaiyán. Su vector de entrada es la distribución de un documento de Word con macros. El RAT parece preparado para desplegar gran cantidad de herramientas, con el fin de exfiltrar información de manera automática, contraseñas, imágenes de cámaras web,... Como objetivo destacable, los atacantes muestran interés por el sector energético, concretamente por los sistemas SCADA relacionados con los aerogeneradores.

Timos en la Apple Store

Sophos detecta 30 aplicaciones en el Apple Store que pretendían suscribir a servicios de pago con extrañas artes y dudosa utilidad. Se anuncian como gratuitas, pero en realidad muestran un periodo de prueba en el que se solicita la introducción de los datos de la tarjeta para activar la app.

Vulnerabilidad en iOS

Se descubre una grave vulnerabilidad en iOS, presente en todas las versiones desde la 6 (septiembre de 2012), permite ejecución de código con solo enviar un email. Y lo que es peor, está siendo aprovechada por atacantes. La versión 13 de iOS resulta un desastre en seguridad.

Ransomware: Ragnar Locker

Para intentar que un ransomware de apenas 50 kilobytes pase desapercibido, los atacantes ejecutan (y descargan) un Windows XP dentro de un VirtualBox (también descargada). Es lo que han conseguido los creadores de Ragnar Locker, especialistas en ransomware contra grandes organizaciones.

Fallo en Sign in with Apple

Se descubre un fallo relativamente sencillo de llevar a cabo en el sistema Sign in with Apple que ha reportado 100.000 dólares a su descubridor. Básicamente permitía que un atacante comprometiese de forma muy sencilla cualquier servicio protegido por Sign in with Apple.

Compromiso de de DigiCert

Atacantes tuvieron acceso a la clave de firma de logs de Certificate Transparency de DigiCert, en lo que puede considerarse el primer caso de compromiso conocido de una estructura de este tipo. Lo consiguen gracias a un fallo en el framework SaltStack.

Vulnerabilidad en Sensormatic Electronics

Johnson Controls notifica al CISA una vulnerabilidad crítica que afecta a varios productos de Sensormatic Electronics, LLC, una subsidiaria de Johnson Controls. La vulnerabilidad provoca que se almacenen en claro las credenciales del usuario que realiza la actualización durante dicho proceso. Uno de los productos afectados es una suite de videovigilancia y alertas: incendio, accesos, ...

Ransomware Tycoon

El ransomware Tycoon utiliza el formato de archivo JIMAGE. Desconocido y poco usado por desarrolladores, sirve para almacenar clases y recursos de múltiples módulos de un JRE. Podría entenderse como un .JAR mucho menos popular. Como nota adicional, le permite ejecutarse en Windows y Linux.

Grave fallo en GnuTLS

Se descubre un grave fallo en GnuTLS. En el handshake TLS se usan dos rondas, pero los tickets de sesión permiten ahorrarse una. El fallo en la implementación de una rotación de claves (STEK) en GnuTLS permitía eludir la generación de tickets, recuperar conversaciones privadas TLS en versiones anteriores a 1.2 y eludir la autenticación en versiones TLS 1.3 (interceptarlas).

106 extensiones maliciosas en la Chrome Store

Se descubren 106 extensiones maliciosas en la Store de Chrome. Su rasgo diferenciador es que todas ellas suponían un esfuerzo coordinado por parte de una compañía de registro de dominios (GalComm), cosa que la compañía niega.

Ransomware Ekans otra vez

El ransomware Ekans (AKA "Snake") ataca de nuevo: Honda obligada a parar varias plantas de fabricación en todo el mundo. Enel, por su parte ve afectadas varias de sus plantas.

Ripple20 afecta a Treck IP

Ripple20: se detectan 19 vulnerabilidades 0-day en la implementación de protocolos Treck IP. Millones de dispositivos estarían afectados, incluyendo dispositivos IoT de proveedores como Intel, Carterpillar, Schnneider Electric, ...

MÓVILES

Apple iOS

Noticias destacables

En el último informe dejamos a iOS 13 en la versión 13.3, con una actualización en diciembre que corregía 15 vulnerabilidades de diversa consideración. Ya en enero de 2020, el año comenzó para iOS con una pequeña revisión, la 13.3.1, que corregía más de 30 CVEs (además de otros fallos de rendimiento y mejoras en usabilidad).

No fue hasta el 24 de marzo cuando Apple liberó la versión 13.4, primera publicación dentro del periodo de confinamiento debido a la pandemia de la COVID-19. **El número de vulnerabilidades corregidas volvía a elevarse hasta la treintena.** Además de los parches incluidos en esta versión, como es habitual, se incluyeron numerosas correcciones y se añadieron nuevas funcionalidades.

El 7 de abril se publicó la versión 13.4.1, que no incluía ningún parche de seguridad, tan solo corrección de errores relacionados con FaceTime y la aplicación Ajustes.

El 20 de mayo de 2020 publicó la versión 13.5 de iOS con un contenido que se estaba debatiendo en la actualidad en relación con el siempre difícil equilibrio entre privacidad y seguridad: **Apple añade un sistema de notificaciones para que las aplicaciones oficiales de rastreo pudiesen notificar a los usuarios de posibles contactos con víctimas de la enfermedad COVID-19**. Además, esta versión corrige hasta 43 nuevos parches de seguridad, muchos de ellos fallos del kernel que posibilitarían la ejecución de código malicioso con los privilegios más altos del sistema.

A modo de curiosidad, podemos ver la referencia a la interfaz de programación de aplicaciones respecto de las notificaciones de exposición a la COVID-19.

El 1 de junio publicó la versión incremental 13.5.1 con un solo parche, el correspondiente a un exploit en el kernel descubierto por el grupo *unc0ver* y que es usado para realizar *jailbreaking* en dispositivos con iOS 13.5; no aplicable en versiones anteriores.

En el horizonte tenemos a iOS 14. La nueva reencarnación del sistema operativo móvil de Apple fue oficialmente presentada en la conferencia (virtual) de desarrolladores WWDC, celebrada el 22 de junio.

En la próxima entrega de este informe, veremos las nuevas capacidades con respecto a la seguridad de iOS 14.

Los exploits de iOS cotizan a la baja

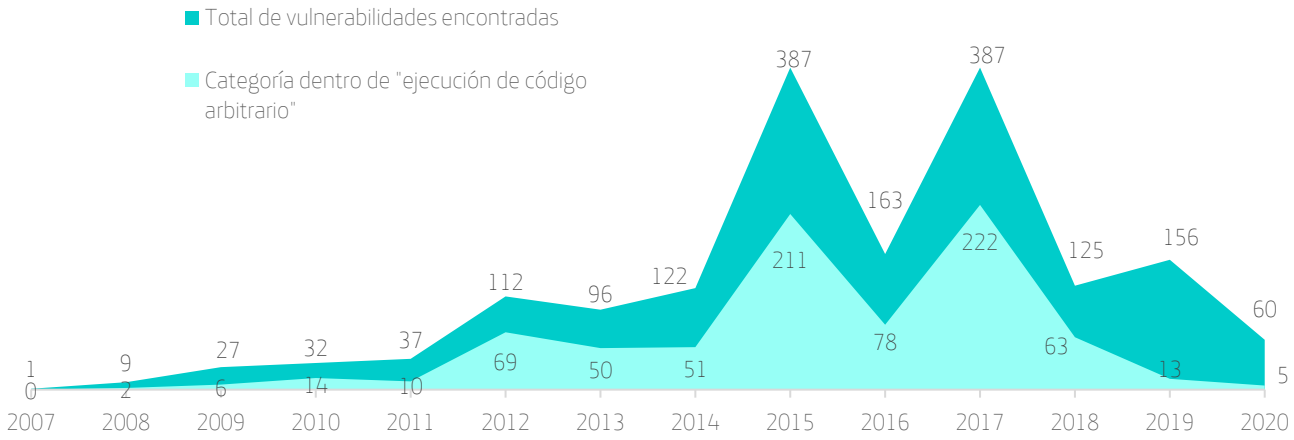
Cabe destacar las declaraciones de la empresa de adquisición de exploits: Zerodium, quienes informaron que suspendían temporalmente la compra de exploits para iOS debido a que estaban recibiendo una gran cantidad. La 13 no ha sido una buena versión para iOS.

Alternativamente, los investigadores pueden enviar sus hallazgos al programa de recompensa de seguridad de Apple, abierto al público desde finales de diciembre del año pasado. Las recompensan varían desde 5.000 al millón de dólares.

gEvolución de vulnerabilidades en iOS durante el primer semestre de 2020

VULNERABILIDADES EN IOS 2020-H1

Evolución de vulnerabilidades por año



En total, **se han parcheado 60 CVEs en el pasado semestre.** De los cuales, 5 poseen la categoría de críticos y permiten la ejecución de código arbitrario. A pesar de representar un descenso en las cifras (a falta de la segunda mitad de año), no ha sido un buen año para la seguridad de iOS. Los fallos se han devaluado por exceso de oferta. **Recordemos que un exploit que permita comprometer por completo un dispositivo de la marca Apple se cotizaba públicamente en 2 millones de dólares.** Actualmente, como hemos comentado en la sección anterior, de forma temporal, Zerodium no acepta exploits para este sistema operativo.

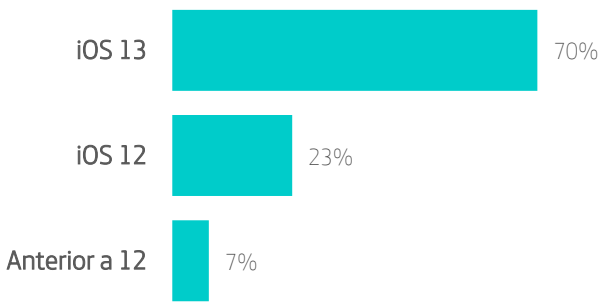
Fragmentación de versiones durante el primer semestre de 2020

Los datos de fragmentación en este semestre revelan una **adopción de la versión actual de iOS 13 del 70%.** Le sigue la versión anterior, 12, con un 23% de instalaciones. Solo un parque de algo más del 7% son instalaciones de versiones anteriores a la 12 y 13 (sobre todo iOS 11 y 10).

La adopción de iOS 13 ha subido 4 puntos porcentuales respecto al periodo anterior. Dos puntos la de iOS 12 y las versiones antiguas bajan 6 puntos porcentuales.

FRAGMENTACIÓN EN APPLE IOS 2020-H1

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.**

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.

Android

Noticias destacables

El 2020 comenzó con un nutrido grupo de parches de seguridad para Android 10. Fue tan madrugador que, como curiosidad, Android se llevó el primer CVE del año: CVE-2020-0001: un fallo que permitía la escalada de privilegios local sin necesidad de la interacción del usuario.

En total, Android ha corregido más de 250 fallos de seguridad de distinta índole, repartidos en seis boletines publicados en la primera semana de cada mes. Esta publicación atañe a la versión de Android AOSP (Android Open Source Project) y ciertos componentes privativos de la versión base.

Los fabricantes conocen las vulnerabilidades con antelación para que puedan disponer de tiempo suficiente en la publicación de los respectivos parches; al menos un mes antes. La idea es que no se demoren en publicar actualizaciones de seguridad en sus respectivas personalización y versiones de Android. Veamos algunas de las más destacadas.

- **BlueFrag:** En febrero se publicó un parche para una seria vulnerabilidad que afectaba a Android 8 y 9, en concreto, al subsistema de Bluetooth. Un atacante podría ejecutar código arbitrario con tan solo acercarse a un terminal que tuviese el Bluetooth activo incluso sin existir un pareo previo. Para fortuna de los usuarios de Android 10, el intento de explotación solo ocasionaba un reinicio del servicio de BlueTooth. Todas las versiones vulnerables han sido parcheadas.

- **StrandHogg 2.0:** Otra interesante vulnerabilidad se dio a conocer a principios del mes de junio. StrandHogg 2.0 es una reedición de una vulnerabilidad ya corregida que afectaba a la forma en la que Android gestiona la multitarea. Aprovechada de la forma adecuada, StrandHogg permitía a una aplicación maliciosa hacerse pasar por una legítima. Esto era explotado para obtener permisos más amplios y disfrutar de mayores privilegios en el sistema.

Libro blanco de la seguridad en Android

En enero se actualizó el libro blanco de la seguridad de Android. Una lectura que expone las mejoras y características de seguridad de la plataforma móvil de Google.

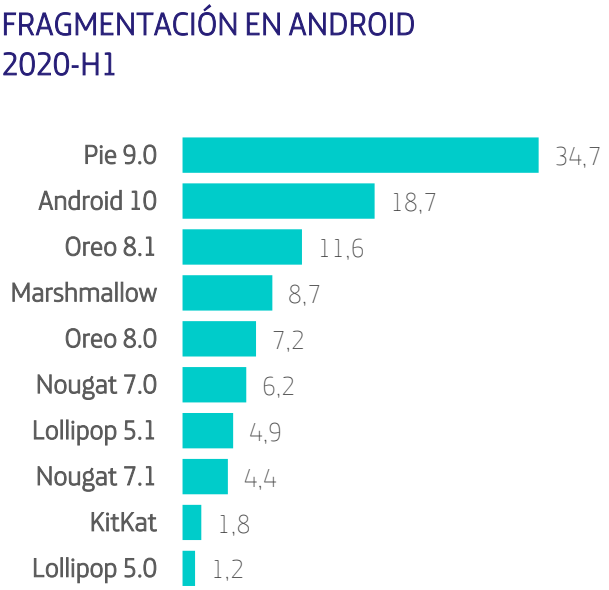
Fragmentación en sistemas Android

Android 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.

Los datos de *statcounter* indican que actualmente solo el 18,69% de terminales Android posee la última versión, Android 10. El grueso sigue siendo su predecesor, Android 9, con una cuota del 34,66%. Les sigue un abanico de versiones desde la 8.1 con un 11,62% y la 8, con el 7,15%, hasta llegar a Android Lollipop 5.0 con, todavía, un modesto 1,2%.

De nuevo revalidamos la afirmación que ya pronunciamos en el informe anterior: **los terminales Android con mayor antigüedad se niegan a jubilarse.** El usuario medio de Android extiende la vida útil de su terminal más allá del tiempo de soporte de parches de seguridad. En definitiva, un riesgo muchas veces no percibido.

Fuentes externas indican que podría haber más de mil millones de dispositivos Android sin cobertura de parches de seguridad.



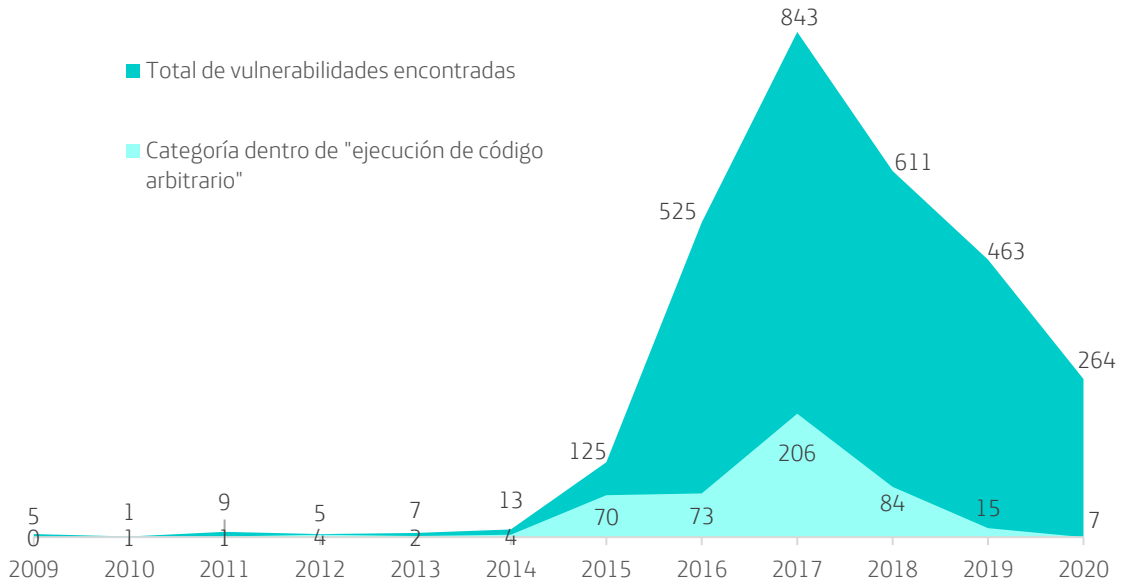
Evolución de vulnerabilidades en Android durante el primer semestre de 2020

En lo que va de año, se han publicado **un total de 264 vulnerabilidades para la plataforma móvil de Google.** Siete permiten ejecución de código arbitrario. **Una vulnerabilidad grave 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.

El número 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 2020-H1

Evolución de vulnerabilidades por año



VULNERABILIDADES DESTACABLES

Comentamos en esta sección algunas de las vulnerabilidades quizás no tan populares, pero notables a nuestro juicio, de este primer semestre de 2020, es decir, aquellas que destacan por su especial relevancia o peligrosidad.

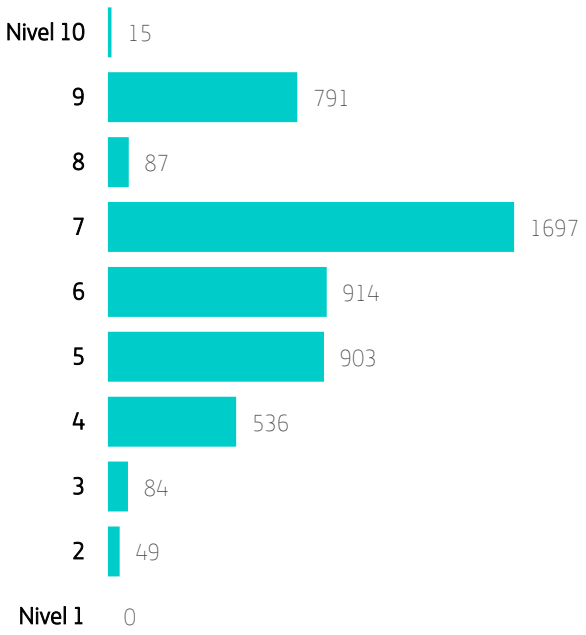
CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2020-0796	Sistema operativo Windows	SMBGhost se trata de un problema de ejecución de código "gusanable" en SMBv3, similar a la explotada por WannaCry pero en otras versiones del protocolo solo presentes en las versiones 1909 y 1903 de Windows 10. Fue anunciado de forma curiosa, solo por Talos y Fortinet, no por Microsoft, durante un breve periodo de tiempo. Parece que tenían acceso a información privilegiada y Microsoft decidió en el último minuto no publicar el parche para este fallo, por lo que estas empresas retiraron el anuncio. Días después publicaría el parche.	10.0
CVE-2020-11896 CVE-2020-11897 CVE-2020-11901	Implementación IP del fabricante Treck	Ripple20 fueron en realidad 19 vulnerabilidades en la implementación de protocolos Treck IP. Como este fabricante licencia su implementación, millones de dispositivos estarían afectados, incluyendo dispositivos IoT de proveedores como Intel, Carterpillar, Schneider Electric... Dentro de este conjunto de fallos, tres vulnerabilidades destacan por su gravedad y alcance.	10.0
CVE-2020-5902		Este fallo se daba en el TMUI de Big IP del fabricante F5. Un sistema que suele estar presentes en el perímetro de las compañías y que se utiliza con muchos fines, habitualmente críticos. Se trata de un Local Traffic Manager y tiene poder total sobre el tráfico que pasa por él. Por tanto el impacto de este problema de ejecución remota de código es más grave de lo que parece puesto que quien lo aproveche tendrá no solo acceso al sistema F5 en sí, sino al servicio que gestiona en la red. Desde un DNS hasta un gestor de certificados TLS, cualquier cosa que esté dentro de esa red. Al poco de anunciar el fallo, se observaron ataques como prueba de concepto y más adelante se hizo público un exploit funcional.	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:

RIESGO DE LAS VULNERABILIDADES

Distribución de vulnerabilidades por riesgo



Top 25 compañías con más CVE acumulados

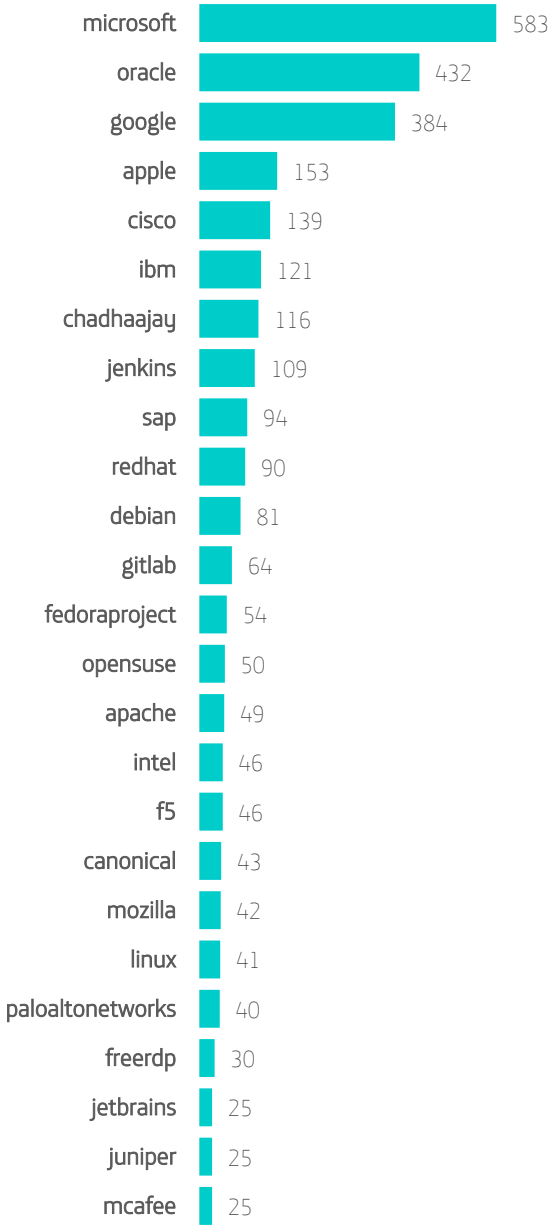
Como en otras ocasiones, hemos de relativizar los datos aquí expuestos, debido a que algunos fabricantes poseen numerosos productos candidatos a obtener un CVE, como puede ser el caso de Oracle y su cuantioso catálogo de productos (alta dispersión). Por el contrario, compañías con un número menor de 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.

Debemos hacer notar también que existen vulnerabilidades con transversalidad. Por ejemplo, Canonical (que es sinónimo de Ubuntu), Debian, FedoraProject, OpenSUSE y RedHat 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.

Aun con todo lo anterior, se observa que hay tres fabricantes destacados: **Microsoft, Oracle y Google**, con estos dos últimos intercambiándose la posición respecto al informe anterior. También respecto al informe anterior, se observa un descenso en el número de CVE acumulados, además de que a partir del 4º clasificado el descenso es mucho más acusado.

VULNERABILIDADES POR FABRICANTE

Top 25 fabricantes por CVE acumulados



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. Esta definición 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.

TOP 10 VULNERABILIDADES

Top 10 CWE más representativos

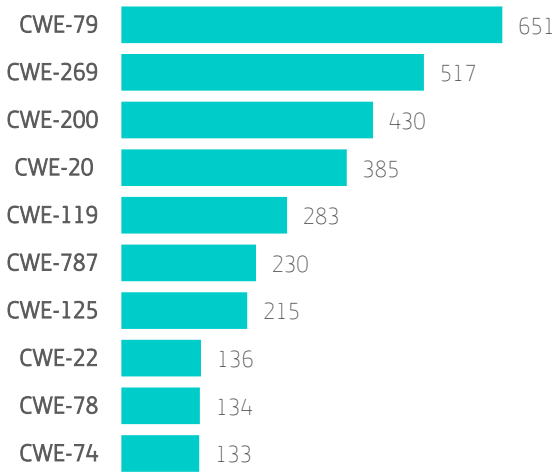


Tabla descriptiva de cada CWE

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.	651
CWE-269	Improper Privilege Management	La aplicación no gestiona adecuadamente los permisos y privilegios otorgados a un usuario.	517
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.	430
CWE-20	Improper Input Validation	Categoría general para errores que consisten en un control deficiente o inexistente en entradas de datos procedentes de usuario.	385
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.	283
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.	230
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.	215
CWE-22	Improper Limitation of a Pathname to a Restricted Directory	Es posible manipular las rutas a archivos que gestiona y usa la aplicación, posibilitando el acceso a recursos protegidos o no relacionados con el ámbito de la aplicación.	136
CWE-78	Improper Neutralization of Special Elements used in an OS Command	La aplicación no valida o filtra de valores o campos procedentes de un componente a otro de la aplicación cuando construye llamadas a comandos del sistema operativo.	134

CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component	Básicamente, se refiere a la no validación o filtrado de valores o campos procedentes de un componente a otro de la aplicación. Esto puede derivar en inyecciones del tipo SQL o vulnerabilidades de inyección en cadenas con formatos.	133

Conclusiones

De nuevo seguimos observando como los ataques relacionados con XSS están en lo más alto, pero en este semestre las debilidades relacionadas con configuraciones inseguras en la gestión de permisos de usuario son las segundas, desplazando a las relacionadas con la falta de control sobre los límites de escritura o lectura de buffers (CWE-119), aquellas relacionadas con la protección de información sensible (CWE-200), o las que se sustentan en insuficiente o deficiente control en los parámetros de entrada en las interacciones con el usuario (CWE-20).

Respecto a estas tres últimas, en términos generales, gaunque desciende sensiblemente el número de debilidades identificadas respecto al anterior semestre, comparado interanualmente (es decir, respecto al mismo periodo del año anterior) se observa que la tasa de descenso es mucho menor.

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 primer semestre de 2020. La fuente de información ha sido principalmente esta página:

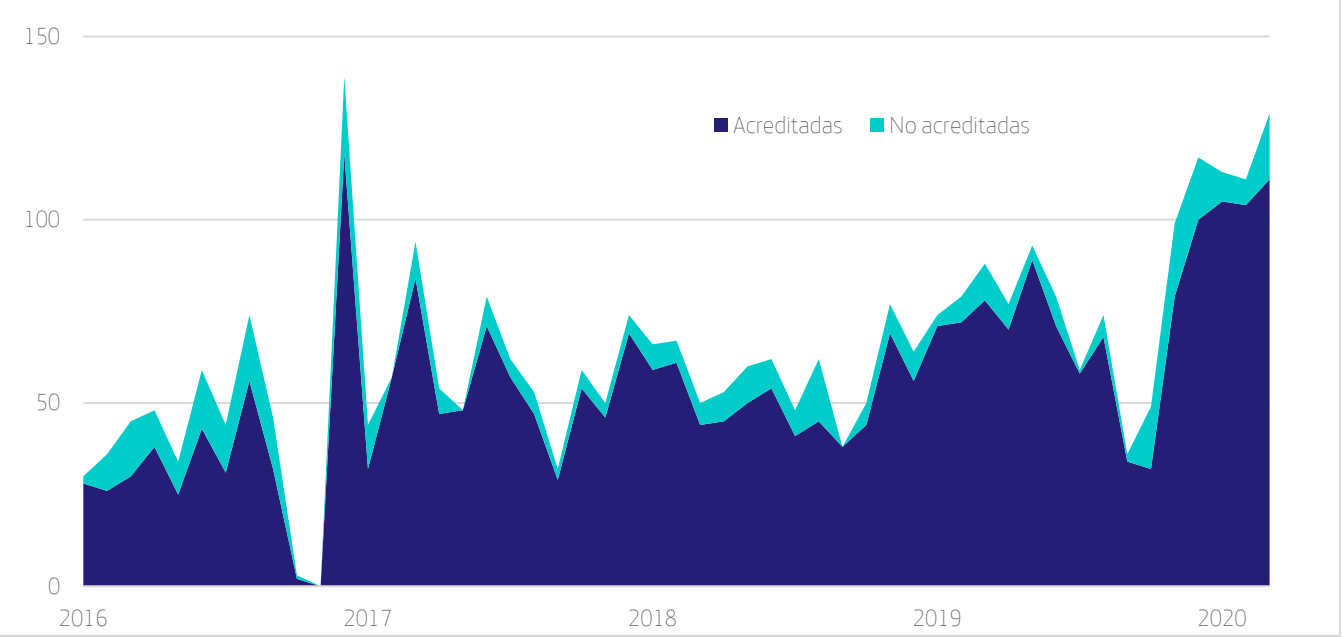
https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments

Estas son las vulnerabilidades acreditadas, esto es, reportadas por alguien identificable, ya sea particular o empresa. En este período hemos analizado 567 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 (más de 600). Entendemos que la mayoría de los fallos no acreditados 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 2020 H1.



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

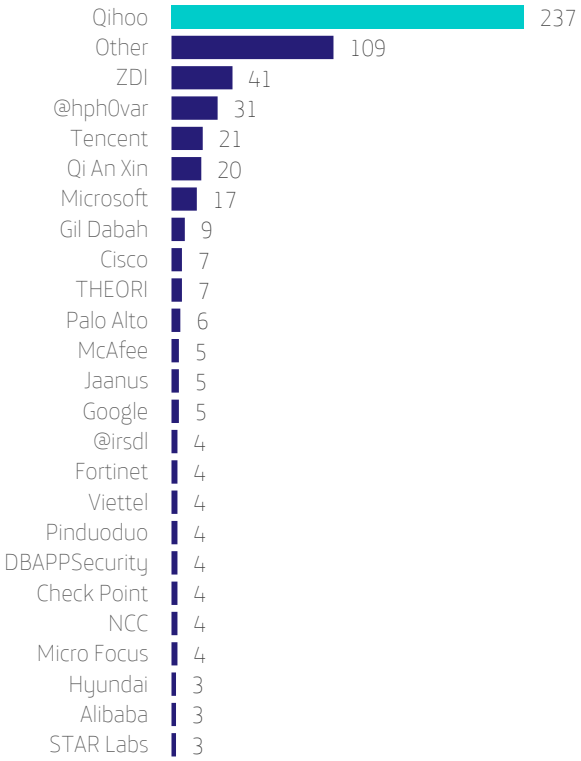
Qihoo es de nuevo la más popular con un total de 237 vulnerabilidades reportadas a Microsoft. Pero con respecto al trimestre anterior, los números cambian sustancialmente.

Qihoo y ZDI reportan más vulnerabilidades

Google cae, y mucho. Si bien el semestre pasado ostentaba el quinto puesto, este semestre ha caído puesto número 14. Microsoft, que era la tercera, cae al sexto puesto. ¿Ha influido la pandemia en los grandes fabricantes? ¿Han dedicado menos tiempo a la investigación de vulnerabilidades? Por el contrario, **Qihoo no solo sigue siendo la primera compañía que encuentra fallos de seguridad en Microsoft, sino que además ha multiplicado sustancialmente su número, de 79 a 237 en este semestre.**

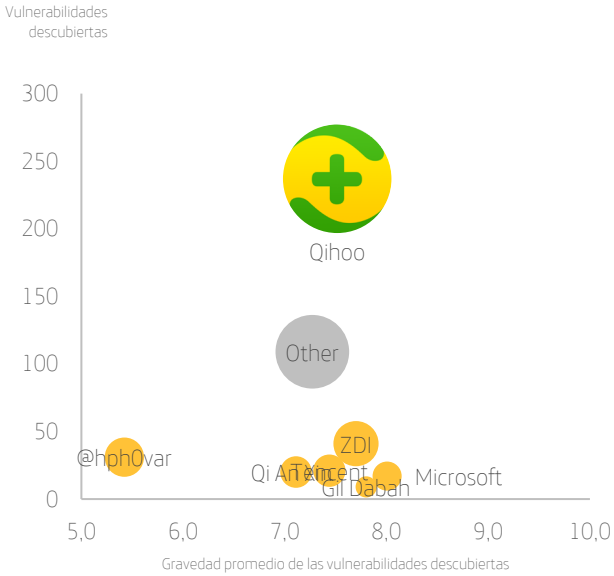
QIHOO ES DE NUEVO LA COMPAÑÍA QUE MÁS VULNERABILIDADES DESCUBRE EN PRODUCTOS DE MICROSOFT

Número total de vulnerabilidades por cada descubridor en el primer semestre de 2020



QIHOO REPORTÓ CASI LA MITAD DE VULNERABILIDADES

Distribución de vulnerabilidades por gravedad y por descubridor; el tamaño de la burbuja es proporcional al número de vulnerabilidades descubiertas durante 2020 H1.



Conclusiones

En un semestre donde todos los meses Microsoft ha rebasado las 100 vulnerabilidades solucionadas, Qihoo ha encontrado 237, muchas más que el trimestre anterior y desplazando sustancialmente a la propia Microsoft y Google, que eran las otras compañías que más fallos encontraban en el software de esta compañía.

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 primer semestre de 2020

En este marco, el virus SARS-COV-2 también ha sido protagonista, como uno de los anzuelos principales en las acciones de los grupos APT. Otros grupos han estado relacionados con el ciberespionaje y otros sencillamente vuelven a la carga con su enésima campaña. Los grupos más destacados en este semestre han sido los siguientes:

Kimsuky (Aka"Velvet Chollima"): por tierra, mar y Office

Este grupo, activo desde 2013, ha utilizado el impacto del COVID-19 para extender su influencia con ataques de spear phishing y documentos de Office . La inyección de templates haciendo uso de la vulnerabilidad CVE-2017-0199 y el uso malicioso de macros han sido sus tácticas preferidas. Este grupo, ha sido relacionado con ataques contra objetivos norteamericanos y surcoreanos, incluyendo centrales nucleares de Corea del Sur en 2014.

Winnti: non stop

Si en el anterior informe hablábamos de este grupo como uno de los más reseñables por su actividad, de nuevo vuelven a colarse en esta selecta lista. Esta vez, utilizando ficheros RTF y un backdoor llamado "Chinoxy" que está basado en otro utilizado por el mismo grupo durante una campaña contra Vietnam, en 2014.

APT32 (Aka "OceanLotus Group"): Truth is out there

Si otros grupos están relacionados con el COVID-19 por haber intentado obtener un rédito del miedo y la confusión de los demás, este grupo supuestamente patrocinado por el gobierno de Vietnam se ha distinguido por haber lanzado ataques contra la administración china, en su búsqueda de información sobre el COVID-19. Al menos, eso es lo que consideran los investigadores de Mandiant, que afirman que dicho grupo ha sido detectado atacando al gobierno regional

de Wuhan y al Ministerio de control de emergencias del gobierno chino intentando recolectar información.

APT39 (aka "Chafer"): una de espías

Este grupo iraní ha sido detectado en una campaña de ciberespionaje contra infraestructuras críticas de Kuwait y Arabia Saudí utilizando un elemento tan importante en la cadena de suministro como los proveedores de telecomunicaciones. Estas tácticas son habituales en el grupo y ya a han ido relacionado con ataques similares en otros países como Turquía en 2014.

PROMETHIUM (aka "StrongPity"): Siempre vuelve

Este grupo, identificado por primera vez en 2002, ha estado de nuevo activo extendiendo su amenaza de suplantación de software entre Europa, América y Asia (Oriente Próximo, India, Vietnam...). Investigadores de Cisco y Bitdefender han logrado rastrear hasta 72 servidores de C&C con distintos objetivos. Los investigadores sospechan de que el vector de entrada es un ataque de "Watering Hole", aunque no pueden confirmarlo. Sin duda, uno de los grandes méritos de este grupo es permanecer tanto tiempo activo, ya que habitualmente grupos tan activos y tan longevos suelen caer salvo que estén patrocinados por estados. Más info.

Bonus Track: La colección de ShadowBrokers sigue dando que hablar

El grupo ShadowBrokers pasó a la historia en 2016 por publicar ficheros de la NSA. Lo que también merece un apunte en la historia es que unos ficheros filtrados en 2016 sigan dando que hablar pasados 4 años. Juan Guerrero-Saade, investigador de seguridad y profesor adjunto en la Escuela de Estudios Internacionales Avanzados de la Universidad Johns Hopkins, ha publicado un estudio en el que afirma que tras algunos de los ficheros filtrados por ShadowBrokers se puede encontrar un grupo no detectado hasta ahora que podría ser de origen iraní. Aunque sólo sea una hipótesis (bien justificada), el hecho de que en este semestre se haya encontrado otro hilo interesante en esta madeja que son los ficheros filtrados por ShadowBrokers, bien merece un espacio en este informe.

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:

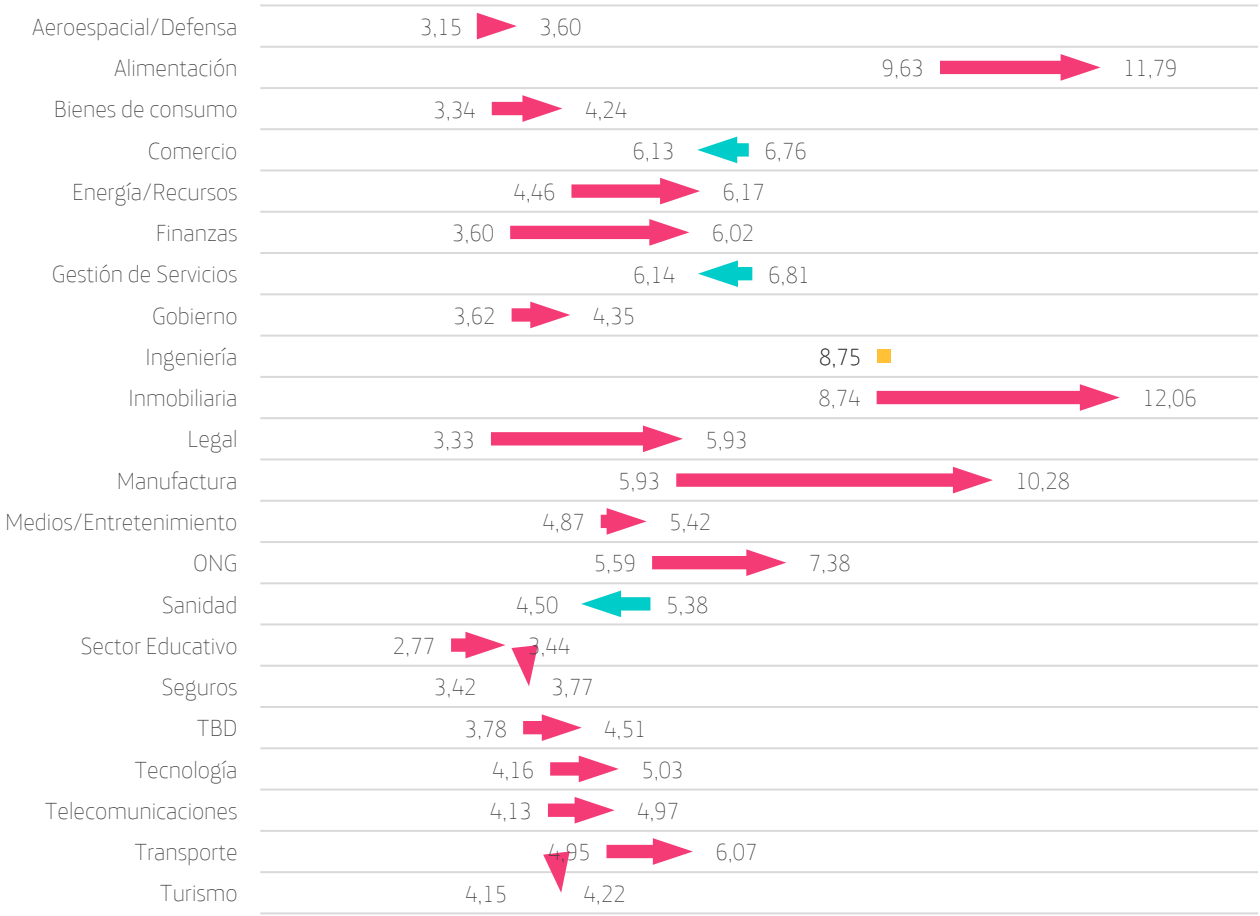
- Tipo de sistema comprometido
- Fecha
- IP de la organización
- Gravedad
- Frecuencia
- Duración
- Confianza

El portal del cliente resume el riesgo de seguridad:

Analítica Ratings Alertas

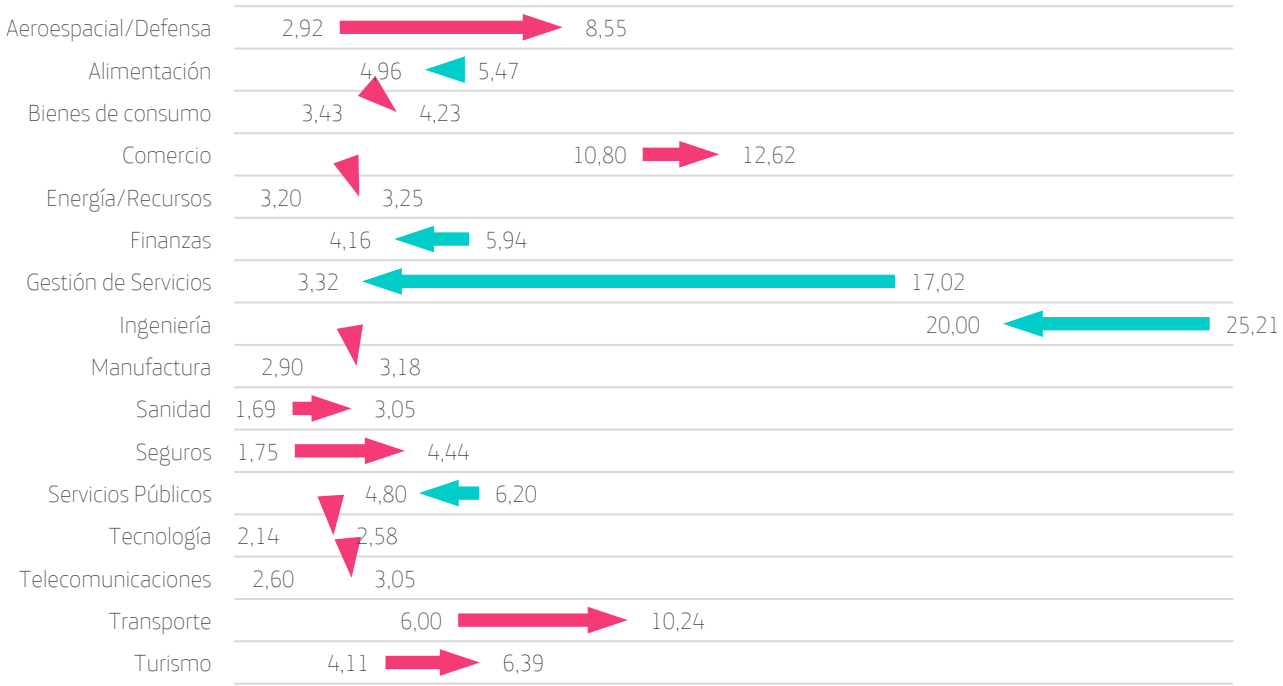
PRÁCTICAS DE SEGURIDAD EN EUROPA

Evolución desde 2019-H2 a 2020-H1 del número medio de **días** efectivos que necesita una **compañía europea** para solucionar una amenaza de malware, agrupado por sector.



PRÁCTICAS DE SEGURIDAD EN ESPAÑA

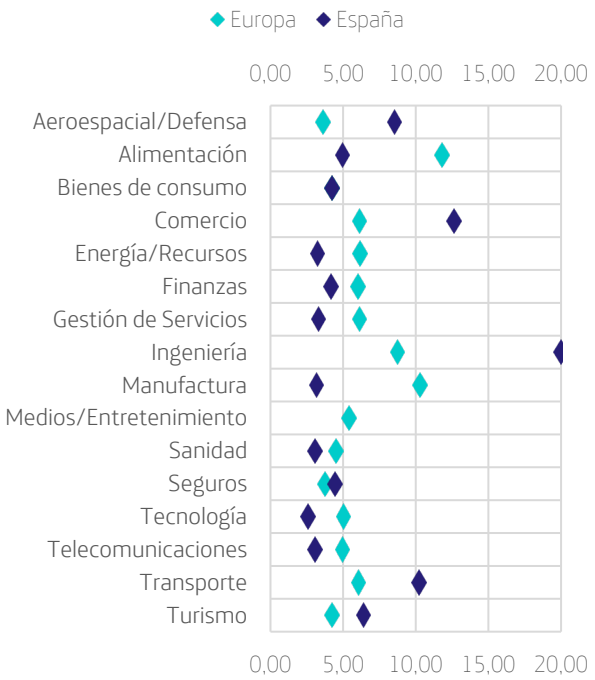
Evolución desde 2019-H2 a 2020-H1 del número medio de **días** efectivos que necesita una **compañía española** para solucionar una amenaza de malware, agrupado por sector.



En estos gráficos hemos visto cómo varía con respecto al semestre anterior la respuesta por sectores. **Destaca la bajada de la "Gestión de servicios" de más de 17 días a poco más de tres.** En el siguiente gráfico compara el tiempo de respuesta entre España y Europa, durante el primer semestre de 2020, agrupado por sector.

COMPARATIVA DETECCIÓN-NEUTRALIZACIÓN ENTRE ESPAÑA Y EUROPA DURANTE 2020-H1 POR SECTOR

Medida en número medio de días



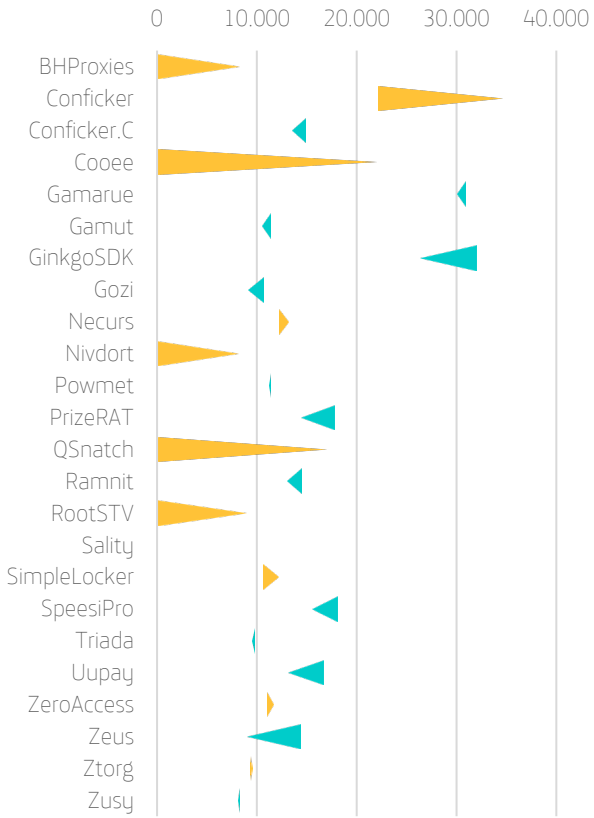
Esto quiere decir, que por ejemplo en el sector del comercio se tardan de media unos 14 días en España en neutralizar una amenaza, mientras que en Europa se emplean unos 7. España en general, necesita una media de días menor con respecto a Europa, para neutralizar un incidente de seguridad.

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-H2 a 2020-H1 medido en sistemas infectados.



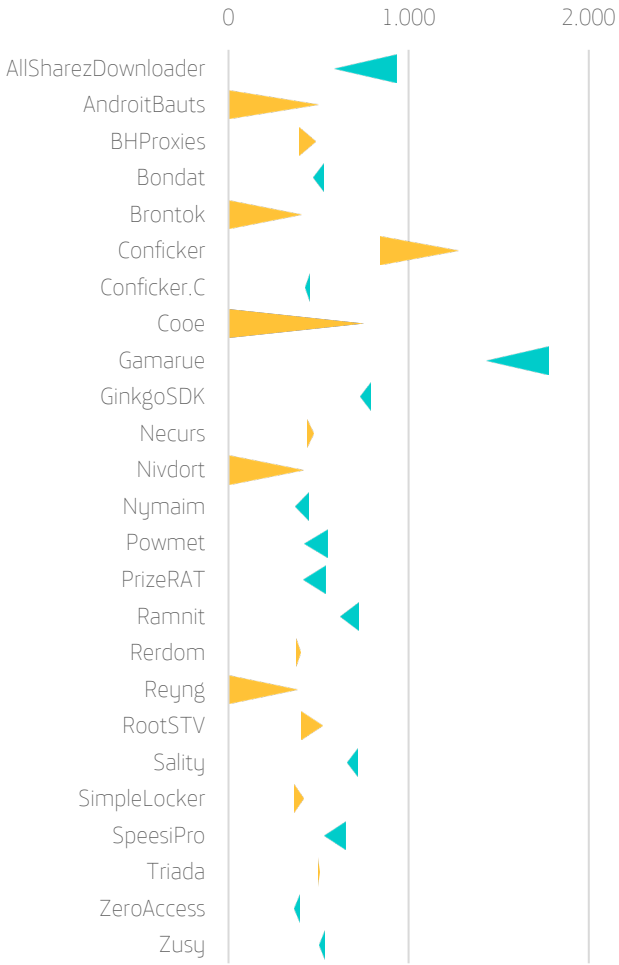
Las 25 familias de malware e infecciones detectadas en España

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.

En España, domina un malware muy diferente al Europeo. Firmas como *AllSharezDownloader* y *AndroidBauts* aparecen en cabeza mientras que en Europa no son representativos.

EVOLUCIÓN DE LAS 25 FAMILIAS DE MALWARE MÁS VIRULENTAS EN ESPAÑA

Crecimiento (en naranja) o decrecimiento (en azul) experimentado desde 2019-H2 a 2020-H1 medido en sistemas infectados.



RECAPITULACIÓN

En el ámbito de la seguridad para móviles, **el alto número de exploits para IOS 13**, la presentación de IOS 14 y la fragmentación de Android han marcado el primer semestre de este año 2020.

Respecto a las **vulnerabilidades y debilidades, se ha podido observar un descenso claro en las cifras de las primeras (sobre todo en las de Nivel 10) pero los tres fabricantes con más CVE asociados siguen siendo los mismos**. Respecto a las debilidades, entran con fuerza aquellas que en las que es clave una configuración de seguridad insuficiente o nula en la gestión de permisos de usuario, permitiendo una escalada de permisos gracias a dicha configuración.

Los grupos APT, por su parte, también han introducido el factor "SARS-CoV-2" en sus operaciones. Unos para sacar provecho, y otros en maniobras de ciberespionaje para descubrir "la verdad" sobre el virus.

En un semestre donde todos los meses Microsoft ha rebasado las 100 vulnerabilidades solucionadas, **Qihoo ha encontrado 237, muchas más que el trimestre anterior y desplazando sustancialmente a la propia Microsoft y Google**, que eran las otras compañías que más fallos encontraban en el software de esta compañía.

De los datos de Bitsight se puede observar que el inquebrantable Conficker vuelve a recuperar el "trono" de las amenazas más virulentas, mientras que también observamos un dato ciertamente preocupante: **en la mayoría de los sectores se aprecia un aumento sustancial de tiempo requerido para neutralizar una amenaza.**

Enlaces de interés

No te quedes sólo en la capa superior del análisis de ciberseguridad, los informes semestrales son acumulativos y resumidos. En el blog de Elevenpaths tenemos mucha más información y noticias que pueden resultar de tu interés. Aquí van los artículos más relevantes en el primer semestre de 2020.

CRIPTOGRAFÍA

RSA contra las cuerdas: 1.001 razones por las que está cayendo en desgracia (PARTE I y PARTE II)
SHA-1 no celebrará más cumpleaños, ha muerto
Criptografía eterna: cómo cifrar los datos hasta el final de los tiempos
Si WhatsApp cifra las comunicaciones, ¿dónde está la clave?
Criptografía Ligera para un mundo doblegado bajo el peso del IoT
OpenPGP: Buscando a Kristian desesperandamente

MALWARE

Apple introduce hasta 14 firmas en XProtect ante la avalancha de malware para Mac
APTualizador (II): deconstruyendo el rootkit Necurs y herramientas para detectarlo y eliminarlo
CARMA, nuestro conjunto gratuito de muestras de malware de Android para investigación
La mayoría del software que trabaja con ficheros no respeta SmartScreen en Windows

PRIVACIDAD

Qué es la privacidad diferencial y por qué Google y Apple la usan con tus datos
Let's Encrypt revoca tres millones de certificados por culpa de un & amp; en su código
Más certificados, más cortos y en cada vez menos tiempo: ¿a dónde va el TLS?
Las "Third Party Cookies" y cómo las maneja cada navegador

CORONAVIRUS

Cómo detectar y protegerse de los phishings del coronavirus
Fake news y ciberamenazas en tiempos de coronavirus
DataCOVID-19: luchando contra el coronavirus con los datos de posición aproximada de tu móvil
20 preguntas sobre las apps de rastreo de contagios del Covid-19
La seguridad detrás de la API de Apple y Google para el seguimiento de contagios de la COVID-19
Criptografía contra el coronavirus
El grupo Vendetta y los emails de phishing de la COVID-19
ElevenPaths Radio – 2×10 Entrevista a Elad Rodríguez

Acerca de ElevenPaths

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

Combinamos la frescura y la energía de una nueva empresa con el conocimiento, el poder y la fuerza de una empresa de telecomunicaciones global para proporcionar soluciones innovadoras que abarcan la prevención, la detección y la respuesta a las amenazas diarias en nuestro mundo digital.

También trabajamos para garantizar un entorno digital más seguro a través de alianzas estratégicas que nos permitan mejorar la seguridad de nuestros clientes, así como a través de colaboraciones con organismos y entidades líderes como la Comisión Europea, CyberThreat Alliance, Cloud Security Alliance, ECSO, EuroPol, Incibe y la OEA .