Telefónica Tech

Informe sobre el estado de la seguridad 2021 H2

Desde la seguridad en móviles hasta el análisis de vulnerabilidades, desde las noticias más relevantes hasta el análisis de la privacidad, comprende los riesgos del panorama actual.

telefonicatech.com

Índex

RESUMEN EJECUTIVO

El objetivo de este informe es sintetizar la información sobre ciberseguridad de los últimos meses (desde la seguridad en móviles hasta las noticias más relevantes 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.

Una de las noticias más destacables no solo del semestre sino del año, se dio en diciembre. El fallo en el software de procesamiento de logs en Java, log4j sufría una vulnerabilidad crítica que no disponía de parche. A partir de aquí, una búsqueda incesante de proyectos que contenían esta librería, nuevas formas de explotación, parches que no eran completos, nuevas vulnerabilidades encontradas... Toda una carrera de obstáculos mientras los atacantes incorporaban estas vulnerabilidades a su conjunto de herramientas de ataque.

Pero este fallo fue más allá y abrió un debate interesante. ¿Hasta qué punto puede un software tan usado, ubicuo y relevante estar mantenido en el tiempo libre de una sola persona? Esta era la situación de log4j. Que además, solo disponía de tres "espónsores" en el github del creador. Poco después se contarían por cientos, pero quizás ya era demasiado tarde. Este incidente hizo recapacitar sobre el papel del software de código abierto en la industria, de cómo los grandes fabricantes lo usan libremente pero no todos aportan a cambio soporte a sus creadores, lo que crea una dependencia muy desequilibrada pero que más tarde puede volverse en su contra: el software heredará los potenciales fallos que introduzca el programador.

Y es que no hay código, libre o cerrado, que sea seguro si no está convenientemente auditado. Y esto requiere recursos.

Este semestre mantenemos nuestra sección especializada en el análisis de amenazas en el ámbito industrial. Esto es posible gracias a nuestro proyecto **Aristeo**, una red de **señuelos industriales** que emplean **dispositivos OT reales** para confundir a los atacantes y extraer la información necesaria para generar inteligencia que fortalezca las defensas de nuestros clientes.

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 SEGUNDO SEMESTRE DE 2021

A continuación, damos cuenta de aquellas noticias que mayor impacto han tenido durante el transcurso de este segundo semestre de 2021.

JULIO

- Los ataques a la cadena de suministro son uno de los puntos de la superficie de ataque más analizados por los ciberatacantes para penetrar en la infraestructura de las organizaciones. El **ataque a Kaseya VSA**, una solución para la monitorización y gestión remota de sistemas es un ejemplo destacado de esta técnica usada por el **grupo de Ransomware Revil que afectó a más de un millón de sistemas solicitando más de 70 millones de dólares americanos para su recuperación**.
- El incidente de seguridad conocido como #printNightmare ha continuado siendo un quebradero de cabeza para los administradores de sistemas windows, el parche KB5005010 liberado por microsoft no cubría todas las versiones de windows y no paliaba el problema de raíz, sino que se limitaba a intentar que no se carguen impresoras por red filtrando la ruta UNC cuando Point&Print está configurado.
- Microsoft vivió también, en este mes, un segundo problema relevante de seguridad conocido como #SeriousSam que afectaba a todas las versiones de windows 10 de los últimos 2 años y medio. Debido a un permiso de lectura para usuario sobre en el fichero SAM y en los archivos que representan las remas del registro SYSTEM y SECURITY, debido a ello un usuario podía acceder a los hashes NTLM de las contraseñas y tratar de crackearlas o utilizarlas directamente cifradas para acceder a sitios de red.
- El 21 de Julio fue detenido en Estepona un ciudadano británico de 22 años, que actuaba online bajo el seudónimo de j0e, y estuvo implicado en el conocido hackeo de cuentas VIP de twitter en 2020. Por otro lado, el atacante que accedió y descargó más de 286.000 fotografías identificativas de una base de datos del gobierno estonio fue también detenido el 28 de julio.
- Nuevas investigaciones realizadas por McAfee Labs indican que documentos no maliciosos están siendo utilizados por actores amenaza para desactivar las advertencias de seguridad antes de ejecutar el código de la macro y así infectar los ordenadores de las víctimas. Se trata de una táctica de ataque que "descarga y ejecuta DLLs maliciosos (ZLoader) sin ningún código malicioso presente en la macro inicial adjunta al spam".
- La red de ferrocarril iraní atacada y fuera de servicio. Los atacantes publicaron en los tablones electrónicos de las estaciones el número del ayatolá Ali Khamenei (líder del país) como teléfono de contacto para los viajeros que quisieran más información sobre la interrupción del servicio (y, por lo tanto, el retraso en sus viajes).
- La empresa sudafricana Transnet, dedicada a actividades de logística, suministro de ferrocarriles, puertos y oleoductos, detenida por un ataque sobre su red de gestión. Entre otras cosas, tuvieron que decretar la condición de desastre mayor y gestionar manualmente la administración de contenedores y el registro de buques del mayor puerto de Sudáfrica, uno de los ejes de la economía sudafricana. Se tardó un mes en recuperar la normalidad del servicio.

AGOSTO

- La vulnerabilidad #PetitPotam, basada en solicitar desde la red interna peticiones SMB al protocolo MS-EFSRPC de la víctima surgió en este mes, la respuesta de Microsoft fue la recomendación de deshabilitar la Web PKI en un dominio. Pero en realidad los problemas raíz son otros: seguir usando protocolo de autenticación NTLM en general, y el hecho de poder conectarte por RPC y realizar las llamadas MS-EFSR sin autenticación.
- Microsoft puso en marcha bajo el nombre de "**super duper secure mode**" (SDSM) un experimento para **incrementar la seguridad del navegador eliminando la compilación Just-In-Time de Javascript.** Esto podría suponer eliminar de un plumazo la mitad de los fallos de seguridad en Edge y otros navegadores. Se trata de una apuesta arriesgada ya que debe medirse muy bien el impacto en rendimiento para los usuarios finales. Veremos en 2022 si sigue adelante la apuesta o se abandona.

- **Un miembro frustrado del grupo de Ransomware Conti publicó el 5 de agosto los manuales de técnicas, tácticas y procedimientos** que utiliza esta organización cibercriminal para formar a sus miembros en como acceder, realizar movimientos laterales y exfiltrar información antes de su cifrado.
- Un atacante lograba robar más de 600 Millones de dólares en criptomonedas de la plataforma de finanzas descentralizadas Poly Network China, lo que convierte este ataque en el más cuantioso a una plataforma de criptomonedas hasta la actualidad.
- El 11 de agosto Accenture reconoce haber sufrido un ataque del grupo de ransomware LockBit, donde se accedió a 6 TB de información y se solicitó 50 millones de dólares a modo de rescate. Accenture anunció que sus sistemas fueron restituidos eficazmente y que la información comprometida no afectaba a sus operaciones ni a los sistemas de sus clientes. Reputacionalmente, puede tener un impacto en su credibilidad como vendedor de seguros de ciberseguridad como sucedió a Axa anteriormente este mismo año.
- En solo 2 días, desde el 19 al 21 de agosto, casi 2000 servidores de correo Microsoft Exchange han sido atacados usando el exploit ProxyShell. Un escaneo lanzado en agosto por ISC SANS, encontró que más del 30%. De los servidores Exchange analizados continuaban sin aplicar el parche de seguridad y por consiguiente seguían siendo vulnerables al ataque cuya prueba de concepto fue liberada públicamente.
- El CISA norteamericano avisa de que la tecnología de BlackBerry QNX es vulnerable al conjunto de vulnerabilidades conocido como “BadAlloc”, que había sido detectado por investigadores de Microsoft 3 meses y medio antes. La tecnología de BlackBerry se utiliza en más de 200 millones de vehículos y sistemas integrados del ámbito industrial, incluidas las infraestructuras críticas y los sistemas de defensa.

SEPTIEMBRE

- En septiembre, el equipo de investigadores de ASSET publicó un total de 16 avisos de seguridad, en los que aborda 20 vulnerabilidades que afectan a la pila de software Bluetooth de placas System-on-Chip (SoC) de once proveedores diferentes. Se estima que los dispositivos afectados rondarían los miles de millones, entre los que se encontrarían dispositivos móviles, equipos informáticos o tablets, entre otros. Entre las vulnerabilidades identificadas destaca la CVE-2021-28139, que permite ejecutar código remoto en
- Dispositivos con placas ESP32 SoC de Espressif Systems a través de paquetes LMP de Bluetooth. Investigadores de QratorLabs han descubierto este septiembre una nueva BotNet con una estimación de 250.000 dispositivos infectados que está detrás de alguno de los ataques más importantes de DDOS del último semestre de 2021. Lanzados contra proveedores de servicios de internet e instituciones financieros de Reino Unido, Nueva Zelanda y Rusia. La particularidad de estos ataques volumétricos es que se basan en saturar la CPU y memoria de los servidores a través de un número elevado peticiones por segundo en vez del uso del tradicional aumento del tráfico basura.
- “El software libre o de código abierto es más seguro por definición porque existen miles de ojos mirándolo y corrigiendo problemas”, esto en un mundo ideal podría ser, pero la realidad es que los fallos están ahí, sea abierto o cerrado. Según un estudio de GitHub se tardan de media cuatro años en detectar un fallo de seguridad, aunque solo un mes en arreglarlo. Para solucionar problemas de seguridad en librerías de código abierto, sobre las que se cimentan cada vez más las aplicaciones de cualquier organización, se ha creado este septiembre el proyecto **Internet Bug Bounty** cuyo objetivo es solucionar vulnerabilidades en proyectos de código abierto con la particularidad que se realiza un reparto 80/20 entre la persona que localiza el error y aquella que finalmente lo soluciona.
- Un investigador ruso bajo el *nick* de IllusionOfChaos, frustrado con el programa *BugBounty* de Apple ha publicado 3 0-days junto a pruebas de concepto para su explotación para iOS que aún están presentes en iOS 15 liberado en septiembre. Los programas *BugBounty* pueden ser una herramienta muy poderosa para el descubrimiento de fallos de seguridad, pero si no se administra de forma correcta puede provocar el efecto contrario cuando los investigadores de seguridad no se sienten respaldados/reconocidos por estos programas.
- Tras la fuga de información proveniente de una base de datos SQL de la plataforma de compraventa de armas en Reino Unido guntrader.uk, en septiembre, un hacktivista de los derechos de los animales ha ido un paso más allá publicando un **mapa geolocalizado de más de 110.000 residencias de los citados poseedores**

de armas creando un potencial problema de seguridad física para sus dueños ya que es un activo muy atractivo para criminales para hacerse con ellas a través de robos domiciliarios.

- En 2021 se ha roto de forma significativa el record de vulnerabilidades zero-day detectadas y explotadas activamente. Aunque esto pudiesen parecer muy malas noticias para la seguridad de la información la realidad es un poco más complicada. También puede indicar la mejora en herramientas defensivas que permiten detectar atacantes "en el acto" o incluso la proliferación de programación de recompensas que permiten descubrir vulnerabilidades a un mayor ritmo que anteriormente. Investigadores del Project Zero de Google mantienen un listado de vulnerabilidades 0-day siendo explotadas activamente desde el 2014.

OCTUBRE

- Un atacante anónimo ha publicado en agosto en el foro 4chan el código fuente e información financiera de los usuarios de la plataforma de streaming de video Twitch. La información incluye más de 5000 repositorios de código fuente e información sensible de las ganancias de los streamers en dicha plataforma desde 2019.
- La NSA ha publicado una advertencia y una serie de recomendaciones para diversas organizaciones americanas como el departamento de defensa y agentes de la estrategia de seguridad nacional contra el uso de certificados wildcard (*.example.com) en sus sistemas ya que su uso facilita ataques para descifrar el tráfico encriptado utilizando una mezcla de protocolos para confundir al servidor. La NSA menciona de forma expresa el ataque conocido como ALPACA (**Application Layer Protocol Content Confusion Attack)** que puede ser explotable en los más de 100.000 servidores web si se combina con el uso de los certificados wildcard.
- El RENAPER de Argentina fue atacado y los atacantes robaron la base de datos con toda la información del DNI de todos los argentinos, incluido el número de trámite del DNI. Se publicaron 60.000 entradas, incluida la información de deportistas como Lionel Messi. El organismo inicialmente lo asoció a un acto interno, pero el Ministerio del Interior del mismo país reconoció que se estaba investigando a las personas con acceso a la base de datos, pero que también se trabajaba con la tesis del robo de claves y que se estaban investigando las conexiones externas.
- El grupo que lanzó REvil contra Kaseya, fuera de combate en una acción del FBI y otras agencias gubernamentales de otros países. La acción consistió en tomar el control de los sistemas del grupo y detenerlos un mes más tarde. Así, el grupo levantó los servicios con una copia de seguridad que estaba comprometida, perdiendo el control de éstos.
- Avast ha descubierto un nuevo ExploitKit para navegadores basados en Chromium. Esto en si mismo es una novedad ya que los atacantes han dejado de lado hace tiempo los ExploitKits para migrar a otro tipos de ataque debido a la fortaleza creciente en seguridad de los navegadores ante estos, por lo que estamos ante la presencia de un "rara avis". La cadena de ataque ha utilizado dos CVEs para escapar al sandboxing del navegador y que permitirían ejecución remota de código en determinados sistemas windows.
- Forbes ha descubierto tras la publicación de un documento en el ámbito de una investigación este noviembre, que en el fraude del CEO cometido a principios de 2020 que concluyó con una transferencia de más de 35 millones de dólares a cibercriminales se usaron técnicas de suplantación de voz a través del uso de sintetizadores *deepfake*. Estas tecnologías se están democratizando cada vez más por lo que tecnologías que hace pocos años podrían atribuirse a películas de ficción son una realidad creciente en el arsenal de los cibercriminales.
- Se ha descubierto, gracias a que Gemini Advisory, una compañía legítima se infiltró en el proceso de contratación, que FIN7 ha utilizado una compañía creada ex-profeso (Combi Security) para engañar a potenciales empleados para realizar un pentesting a organizaciones públicas como prueba de sus capacidades para entrar a la compañía. El grupo FIN7 ya había usado un método similar a mediados de 2020 con una empresa falsa llamada Combi Security. Se trata principalmente de un asunto de costes para la organización cibercriminal, ya que es más barato contratar a alguien que usar los foros de la DarkWeb para contratar a expertos en pentesting que conocen las ganancias que pueden obtenerse de un pentesting exitoso y delictivo.

NOVIEMBRE

- El mayor repositorio de paquetes node.js ha corregido en noviembre un error que permitiría a un agente amenaza publicar versiones de cualquier paquete sin autorización previa. Según Github, no había registros de actividad relacionados con la explotación de este fallo, si bien es cierto que este pasado 4 de noviembre se detectaron versiones vulneradas de las librerías NPM “coa” y “rc”, con más de 23 millones de descargas semanales en conjunto, con malware inyectado.
- El FBI (Federal Bureau of Investigation) emitió un comunicado el pasado 13 de noviembre en el que confirmaba que un error de configuración habría permitido a un actor malicioso el acceso temporal a uno de sus servidores de correo. Como consecuencia del acceso no autorizado, el atacante habría enviado correos de spam desde el dominio @ic.fbi.gov donde comunicaban una posible intrusión en los sistemas del FBI. El FBI asegura que no se habría accedido a información sensible ni a datos PII.
- El pasado 26 de noviembre, la empresa con sede en Japón, Panasonic, confirmó un acceso no autorizado a su red detectado el día 11 de noviembre. Atendiendo a fuentes locales, los atacantes habrían mantenido el acceso durante cuatro meses desde junio hasta noviembre. Entre los datos expuestos se podría encontrar información de clientes y empleados, así como, supuestamente, archivos técnicos vinculados a la operativa de la empresa nipona.
- Hewlett Packard ha lanzado el 1 de noviembre una actualización de seguridad tras el descubrimiento por parte de la firma finlandesa F-Secure de una vulnerabilidad, con código CVE-2021-39238 que afectaría a más de 150 modelos de impresoras multi-función que permitiría un ataque de tipo gusano que pudiese propagarse por red interna o internet.
- Rolling Stone y Property of the People obtuvieron un documento del FBI que detalla exactamente qué tipo de información puede obtener el FBI de varias aplicaciones de mensajería con una orden judicial. Y resulta que WhatsApp e iMessage proporcionan la mayor cantidad de información. WhatsApp, iMessage y Line brindan contenido de mensaje "limitado" en respuesta a una solicitud legal del FBI. Sin embargo, Signal, Telegram, Threema, Viber, WeChat y Wickr no revelan ningún contenido de mensaje.
- GoDaddy ha sufrido y detectado el 17 de noviembre una filtración de información que afecta a más de 1,2 millones de clientes de su servicio de hosting de wordpress gestionado. La información a la que el atacante ha tenido acceso incluye la password original del servicio, los usuarios y contraseñas de acceso sFTP y de las bases de datos, y un subconjunto de claves privadas SSL. GoDaddy ha reseteado las contraseñas de los clientes cuyo servicios han sido impactados y estaba trabajando en la generación de nuevos certificados SSL para aquellos clientes afectados.
- El nuevo conjunto de vulnerabilidades en el protocolo Bluetooth, BrakTooth descubierto en septiembre, preocupa especialmente por su potencial impacto en todos los dispositivos que usan dicho protocolo. En este mes se presentaron los resultados de una prueba de concepto sobre la explotación de dichas vulnerabilidades, provocando que agencias y organismos por todo el mundo insistieran en su peligrosidad. Una de ellas (CVE-2021-28139) afecta especialmente a dispositivos industriales y podría poner en riesgo la seguridad de las personas y a las infraestructuras críticas.

DICIEMBRE

- Apple lanzó a principios de 2021 su producto AirTag que permite la localización de objetos perdidos a través de bluetooth o usar el conjunto de dispositivos apple global para localizarlo cuando está fuera de rango. Siendo una gran idea varios expertos en privacidad mostraron su preocupación por el posible mal uso de esta tecnología para localizar inadvertidamente a personas. En diciembre saltó la noticia en San Francisco del citado mal uso para el robo de vehículos de alta gama.
- Un investigador de seguridad ha descubierto que un misterioso actor amenaza con nick KAX17 sería el propietario desde 2017 de más de 1000 servidores dentro de la red Tor especializada en la anonimización de tráfico. Lo más probable es que el atacante esté tratando de desanonimizar e identificar usuarios de la red Tor. Se trata de un atacante con abundantes recursos y conocimiento por lo que podría estar apoyado por

un gobierno. Mantenedores de la red Tor han eliminado en octubre y diciembre de este año cientos de servidores atribuidos a KAX17.

- El fabricante de coches Volvo ha reconocido en un comunicado en diciembre haber sufrido una intrusión en sus servidores de alojamiento de ficheros que habría resultado en la extracción de información confidencial relacionada con su I+D. La filtración de este tipo de información puede resultar altamente dañina para Volvo por ejemplo si incluye documentos confidenciales y con sensible propiedad industrial como aquellos relacionados con su negocio en el sector de los coches eléctricos.
- El conocido gestor de contraseñas LastPass confirma que en diciembre se produjo un intento masivo de *credential stuffing* contra sus usuarios desde una IP de Brasil. Decenas de usuarios publicaron en Twitter noticias relacionadas lo que podría evidenciar un ataque de filtración de información, sin embargo, LastPass ha comunicado que no tiene constancia de ninguna fuga de información confidencial por lo que apunta a un intento de reutilización de credenciales de otros servicios.
- Un grupo de cibercriminales especializados en Ransomware-as-a-service y bautizado con los seudónimos de Alphb y BlackCat puede ser considerado el primer grupo que utiliza de forma exitosa malware basado en el lenguaje de programación Rust tras la publicación en 2020 de una prueba de concepto de una cepa de malware en este lenguaje. Diversos Investigadores de seguridad confirman que el ransomware es altamente sofisticado, por lo que habrá que estar atentos a sus actos en 2022. Esto también denota una tendencia de creadores de malware de moverse a lenguajes considerados más seguros como *Rust* frente a los más tradicionales como C y C++.
- Conocida como Log4Shell, el impacto del conjunto de vulnerabilidades que han ido apareciendo en la librería de código abierto Log4j, estándar de facto para registro de información de aplicaciones Java no para de crecer. La vulnerabilidad, que permite la ejecución remota del código escrito en los logs y se ve favorecida por la función JNDI (Java Naming and Directory Interface), que permite la llamada a servidores externos para la ejecución de código, resultando en la potencial ejecución de código desconocido especialmente manipulado y en la instalación de malware. Se descubre adicionalmente que la vulnerabilidad Log4Shell también afecta a fabricantes de sistemas de control industrial. El rango de productos cubre varias tipologías de aparatos y se extiende por todas las verticales industriales. Google ha barrido el repositorio central de Maven y ha detectado más de 35000 librerías vulnerables al ataque a través de su dependencia directa o indirecta de Log4j. Dos miembros del equipo Google Open Source Insights comentan que cuando habitualmente un fallo grave en Java afecta a un 2% del índice central de Maven, en el caso de Log4Shell esto sube hasta el 8% por lo que podríamos estar ante varios años hasta que la vulnerabilidad sea totalmente erradicada.

MÓVILES

Apple iOS

Noticias destacables

Dejamos el año 2021 con iOS 15.2. Ha sido un semestre en el que, como viene siendo habitual, se ha publicado una revisión mayor de la versión de iOS: hemos pasado de la 14 a la 15. Como todo cambio de versión, nos trae novedades tanto en las funcionalidades del sistema como en nuevas características de seguridad y parches de vulnerabilidades.

No obstante, retrocedamos a mediados del año, donde dejamos el informe anterior. En julio, se publicó un importante boletín que corregía una peligrosa vulnerabilidad que estaba siendo explotada por diferentes actores, un *zeroday* en toda regla. Además, la situación se complicó con la publicación en Github de un exploit. Por ello, el 26 de julio se libera iOS 14.7.1 y se conmina a los usuarios de la plataforma móvil de Apple a actualizar sus dispositivos con urgencia.

Tras un mes de agosto relativamente tranquilo, septiembre inauguró el curso con iOS 14.8 que venía cargado con una mochila de 14 parches, la mitad de ellos tapando agujeros por los que se podía ejecutar código arbitrario. Esta fue la última actualización de la versión 14 de iOS.

iOS 15

Una semana después de 14.8 se libera la esperada nueva versión de iOS, la 15. Además de las nuevas funciones venía cargada de numerosos parches de seguridad, hasta 39, casi un tercio evitaban nuevas formas de ejecutar código arbitrario.

iOS 15, en línea con las últimas características de seguridad añadidas en versiones recientes, incluía nuevas medidas de seguridad englobadas en el capítulo de la privacidad. No obstante, se trata en su mayoría de medidas adoptadas en sus aplicaciones por defecto: *Mail, Safari, iCloud*, etc. Por ejemplo, *Mail* incluye ahora un mecanismo para evitar el seguimiento por la técnica conocida como *tracking pixel* o pixel de seguimiento. Una imagen de 1x1 (es decir, un pixel) que al ser solicitada permite recabar datos de navegación.

Octubre no fue un mes tranquilo. Se liberaron dos parches de urgencia, el 15.0.1 que permitía ver contenido privado o sensible desde la pantalla de bloqueo del terminal. Días después se publicaba 15.0.2, la cual contiene un parche para un nuevo *zeroday* que estaba siendo explotado.

Ya finalizando un vertiginoso octubre, se libera 15.1, la primera gran actualización de la rama 15. Este grupo de parches contiene 22 correcciones, media docena correspondiente a vulnerabilidades que podrían causar la temida ejecución de código arbitrario.

Curiosamente, aunque hubo un 15.1.1, esta versión no contenía material de seguridad, por lo que 15.1 no supuso más sobresaltos de seguridad. Aun así, Apple cerró el año con un 15.2, que contenía hasta 42 parches con una docena de ellos tapando agujeros por los que se podrían colar ejecuciones de código arbitrario.

Evolución de vulnerabilidades en iOS durante el segundo semestre de 2021

Un exploit que garantice la ejecución remota de código arbitrario en iOS se sigue cotizando a dos millones de dólares. Medio millón por debajo de su equivalente Android.

El segundo semestre de 2021 se ha cerrado con 120 vulnerabilidades parcheadas, de las cuales, 40 son consideradas de alto riesgo, con posibilidad de ejecutar código arbitrario. Algunas de ellas afectan al propio núcleo del sistema

Fragmentación de versiones durante el segundo semestre de 2021

Como es tradición, la fragmentación nunca ha sido un problema para los desarrolladores de iOS. La ventaja de contar con una plataforma homogénea es incontestable y continúa arrojando cifras casi calcadas cada vez que revisamos la adopción por parte de los usuarios de iPhone de una nueva versión del sistema operativo.

A fecha de cierre de este informe, no se disponía de datos de fragmentación de versiones por parte de Apple, por lo que las cifras que relatamos a continuación proceden de StatCounter.

La nueva versión de iOS, la 15, alcanza un segundo y tercer puesto con un 34% de cuota. Es algo que suele repetirse como un patrón, la adopción en masa eleva la nueva versión a una buena cuota, pero sin destronar a la versión anterior, sin embargo, como probablemente veamos en la siguiente entrega de este informe, las cifras se alternarán y veremos un cambio en las posiciones con el declive de la versión anterior.

iOS 14.8 todavía se corona con el primer puesto con el 32.24%. Además, sus versiones anteriores, 14.7, 14.6, 14.4, todavía arañan otro 20%.

El último terminal soportado por iOS 15 es el iPhone 6S, un modelo que se estrenó el 25 de septiembre de 2015, hace más de seis años.

FRAGMENTACIÓN EN APPLE IOS 2021 -H2

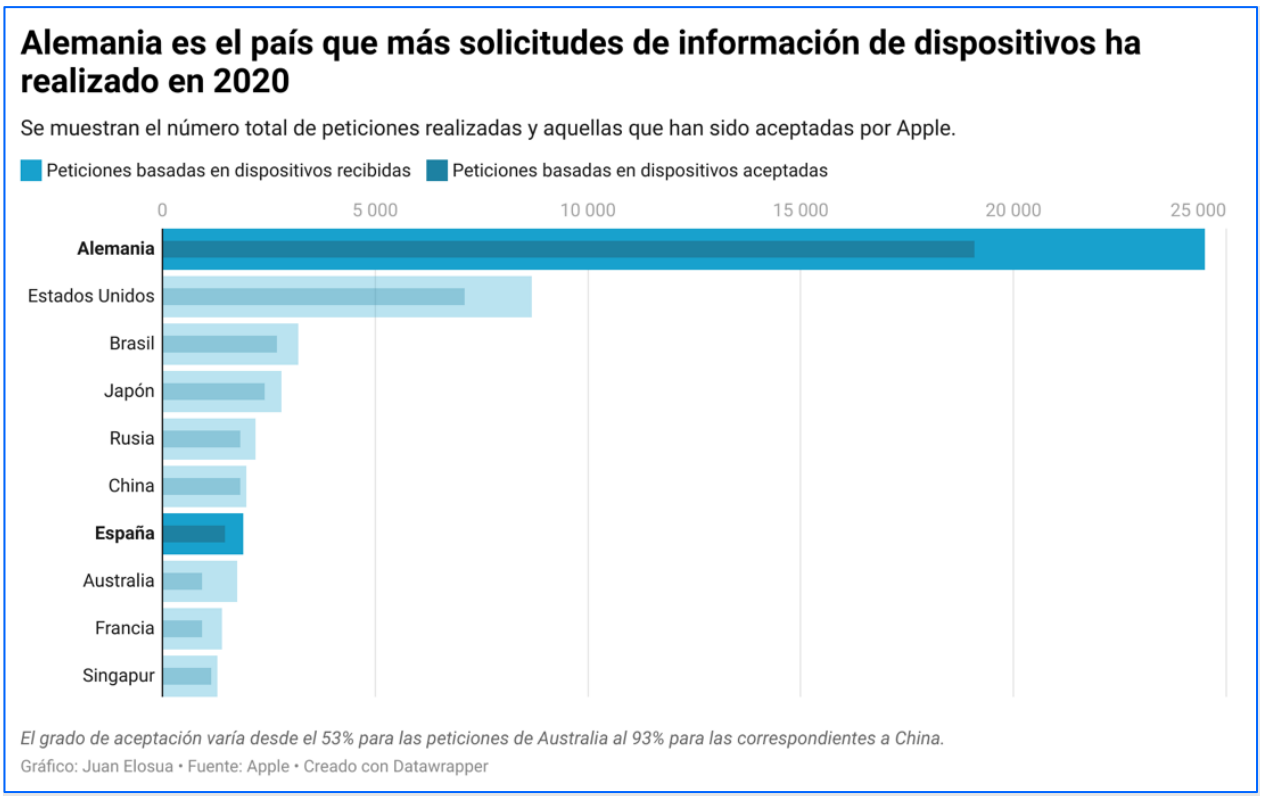
iOS 14,8	32,24%
iOS 15,1	17,37%
iOS 15	16,55%
iOS 14,7	10,05%
iOS 14,6	4,37%
iOS 14,4	4,03%

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. Actualizamos aquí algunos datos que hemos extraído de la información publicada por Apple para el año 2020 sobre las actividades y peticiones de los gobiernos a la compañía.

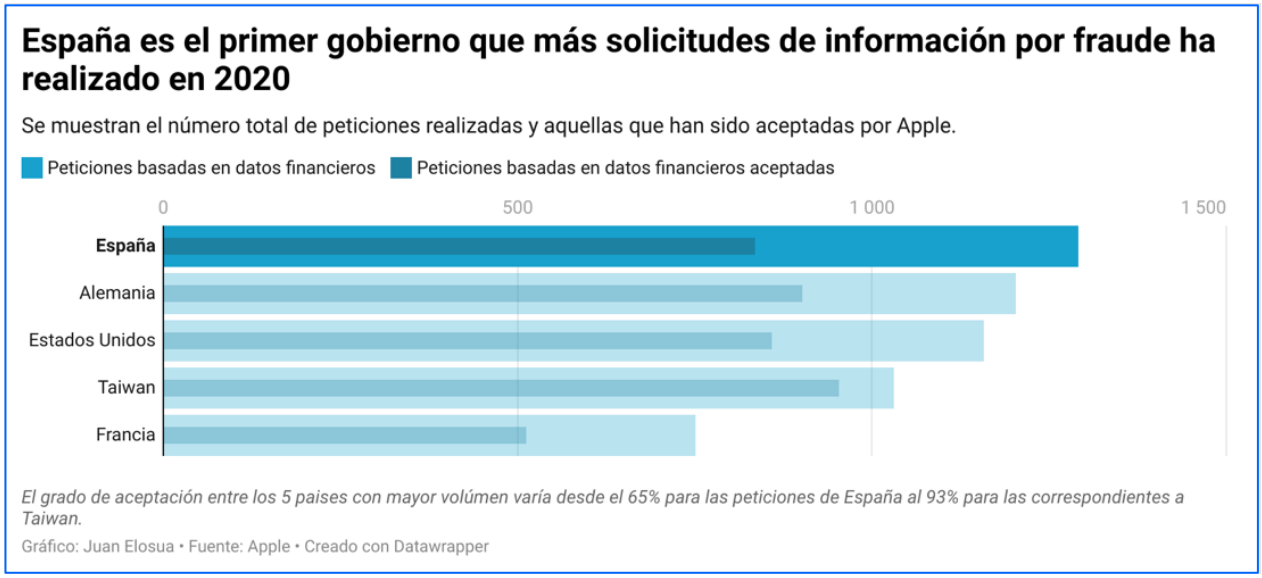
Peticiones basadas en dispositivos

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.



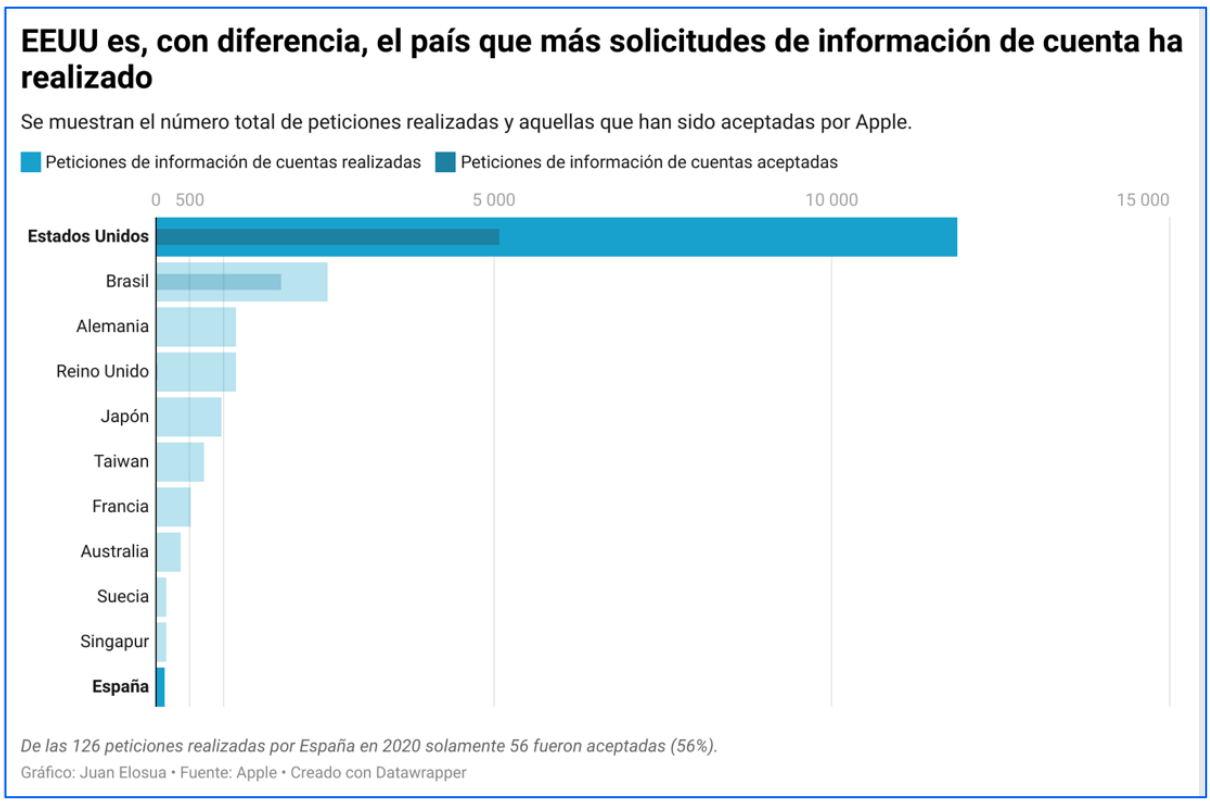
Peticiones basadas en datos financieros

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.



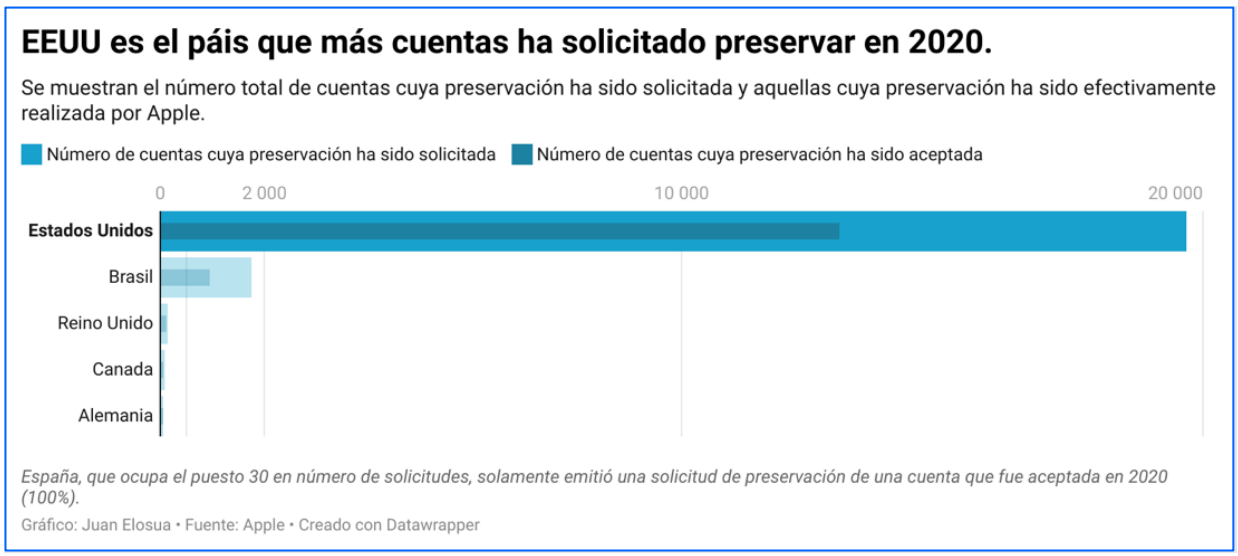
Peticiones basadas en cuentas

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…).



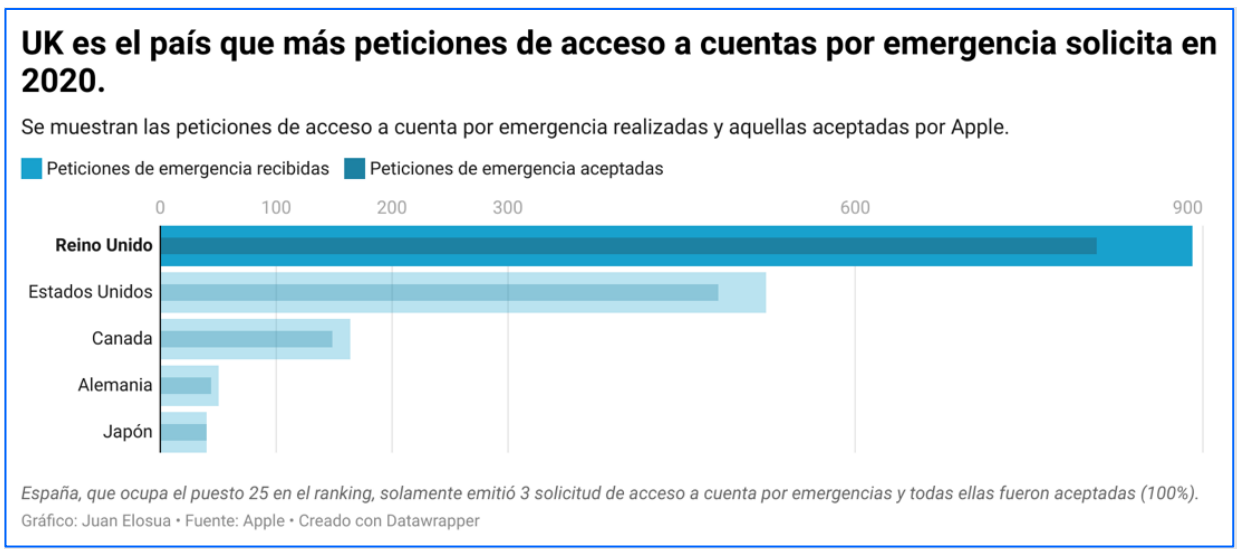
Peticiones relacionadas con la preservación de cuentas

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.



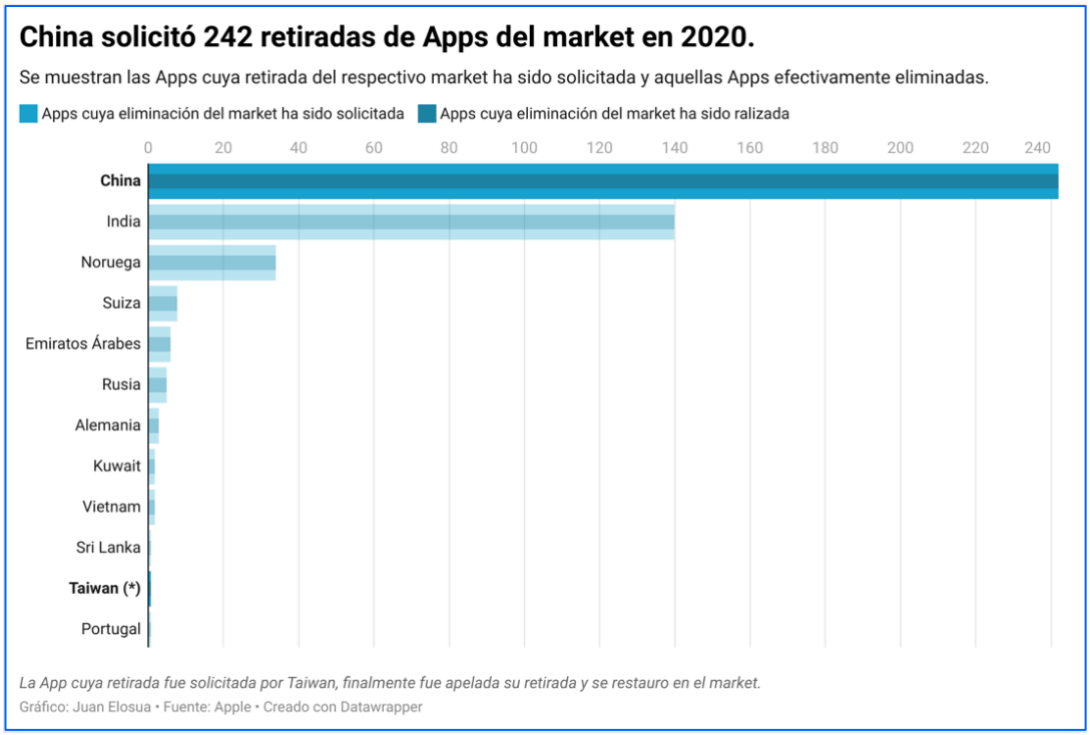
Peticiones por emergencias

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.



Peticiones relacionadas con la retirada de apps del market

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



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 gobierno alemán es el que más solicitudes ha generado para obtener información sobre dispositivos.
- España es el país que más solicitudes de información de cuentas por fraude ha realizado en el año 2020.
- Estados Unidos solicita con diferencia más que cualquier otro país la preservación de cuentas y el acceso a los datos alojados en ella.
- De manera poco sorprendente, China es el país que más retirada de apps solicita en el App Store.

Aclaración: en este ejercicio hemos representado en gráficas las tablas que publica la propia Apple. Es importante especificar que las peticiones se realizan por lotes que pueden incluir más de una cuenta o dispositivo. Por ejemplo, Apple contabiliza el número de peticiones de información de dispositivos, y a su vez cada petición puede contener un número indeterminado de dispositivos 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 dispositivos entre todas las peticiones y luego dice que ha satisfecho el 90% de las peticiones, no sabemos cuántos dispositivos individuales se han proporcionado. Por lo que se trata de un ejercicio que puede aportarnos una idea aproximada de la cantidad real de dispositivos proporcionados para el ejemplo expuesto.

Android

Noticias destacables

En octubre de 2021, se libera la versión 12 del sistema operativo Android, tras su anuncio, un año atrás. Esta versión trae ciertas mejoras en la privacidad, como el indicador de uso de la cámara y micrófono. Es decir, cuando una aplicación haga uso activo de estos periféricos se indicará mediante un icono en la barra de estado.

Otra de las mejoras ha sido la incorporación de una opción menos agresiva para la geolocalización del usuario. Ahora, el usuario podrá optar por una geolocalización aproximada en contraposición a una precisa. Es una opción útil cuando queremos hacer uso de aplicaciones que necesitan posicionarnos y valoramos que con una posición aproximada es suficiente.

Además, se incorpora un cuadro de mandos de privacidad en el que el usuario podrá tener una perspectiva general del uso que producen las aplicaciones respecto de los distintos usos que pueden darse de nuestros datos. En este, podremos ver que aplicación y cuando hizo uso de la cámara, acceso a archivos, etc.

Por último, otra de las grandes bazas en seguridad es la incorporación de un sistema denominado *Private Compute Core*. Se trata de un subsistema en el que el procesamiento de los datos se aísla de los servicios y aplicaciones, impidiendo el acceso a estos datos salvo que el usuario de su consentimiento de forma explícita.

En total, se han publicado 250 parches para corregir diversas vulnerabilidades repartidos en seis boletines, los correspondientes a cada mes del semestre pasado. De esos 250 parches, 29 corrigen vulnerabilidades que han sido calificadas de críticas y podrían facilitar la ejecución remota de código arbitrario.

Fragmentación en sistemas Android

Android no publica estadísticas que muestren el estado de fragmentación entre versiones. Los datos obtenidos pertenecen a fuentes públicas, es decir, no están contrastados con las fuentes oficiales.

La última publicación de *Statcounter* a fecha de edición de este informe nos indican que la versión más implantada de Android es la 11, con un share del 35.35%, seguida por la 10 con un share de 27.02%. Recordemos que 11 arrancó el semestre anterior con un share del 15%, lo cual representa un incremento de cuota importante.

Tradicionalmente, el ecosistema Android tarda tiempo en propagar las nuevas versiones, dado que los fabricantes han de adoptarlas a sus propias compilaciones, con aplicaciones y servicios inherentes a las distintas marcas.

La porción restante se la reparten las versiones inferiores a la 10, donde ninguna supera el 10% de mercado salvo la versión 9, que aún supone el 13.46% del mercado. La versión más antigua de Android con cuota significativa, un 3.2%, es Android Nougat o 7.0, un sistema que fue lanzado en agosto de 2016.

FRAGMENTACIÓN EN ANDROID 2020 -H2

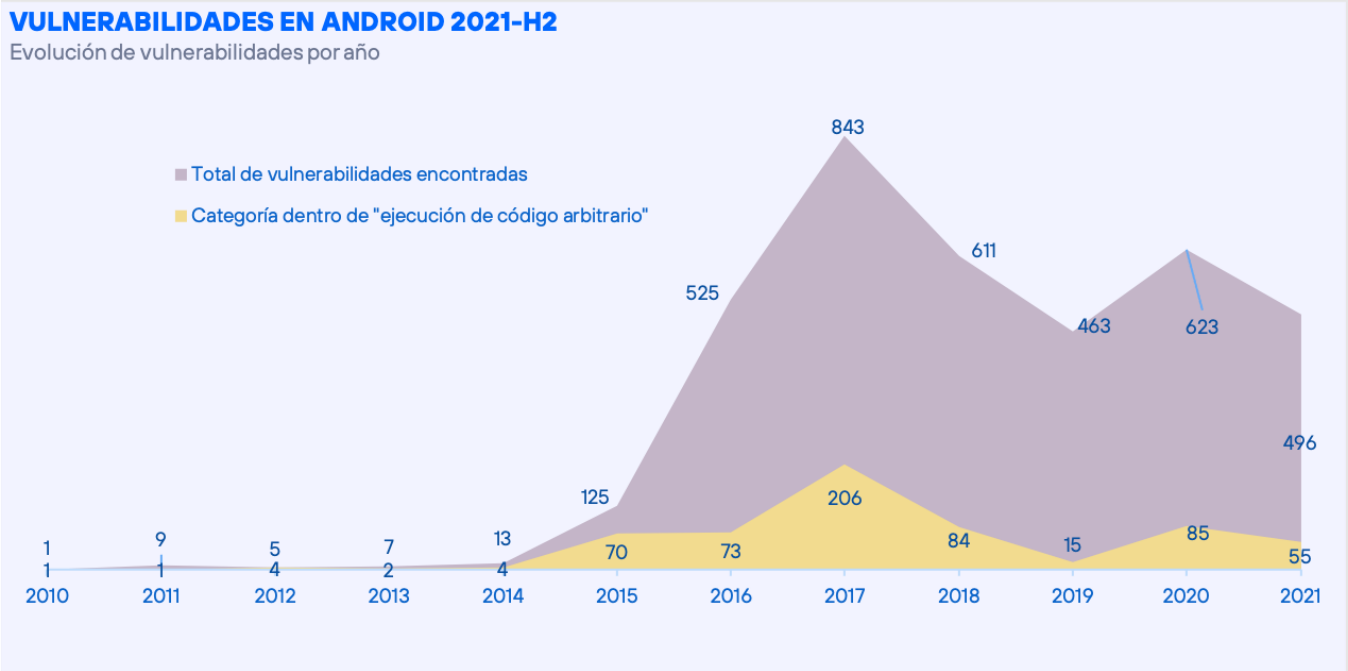
11	35,35
10.0	27,02
9.0 Pie	13,46
8.1 Creo	9,11
7.0 Nougat	3,2

Evolución de vulnerabilidades en Android durante el segundo semestre de 2021

Un exploit que garantice la ejecución remota de código arbitrario en Android continúa cotizando a dos millones y medio de dólares. No hay cambios respecto a la cifra de remuneración desde hace bastante tiempo.

Típicamente, Google libera un grupo de parches se seguridad cada mes. Por lo que han sido publicados seis boletines que suman un total de 250 CVEs o vulnerabilidades corregidas ese semestre. 29 de ellas críticas. Cifras muy similares al conjunto del semestre pasado. En la gráfica se observa lo acumulado durante 2021.

No obstante, muchos de estos fallos afectan a software o firmware de ciertos fabricantes en particular, lo que significa que una misma vulnerabilidad no tiene por qué afectar a todo el parque de dispositivos Android, sino tan solo a aquellos con lo componentes afectados.



VULNERABILIDADES DESTACABLES

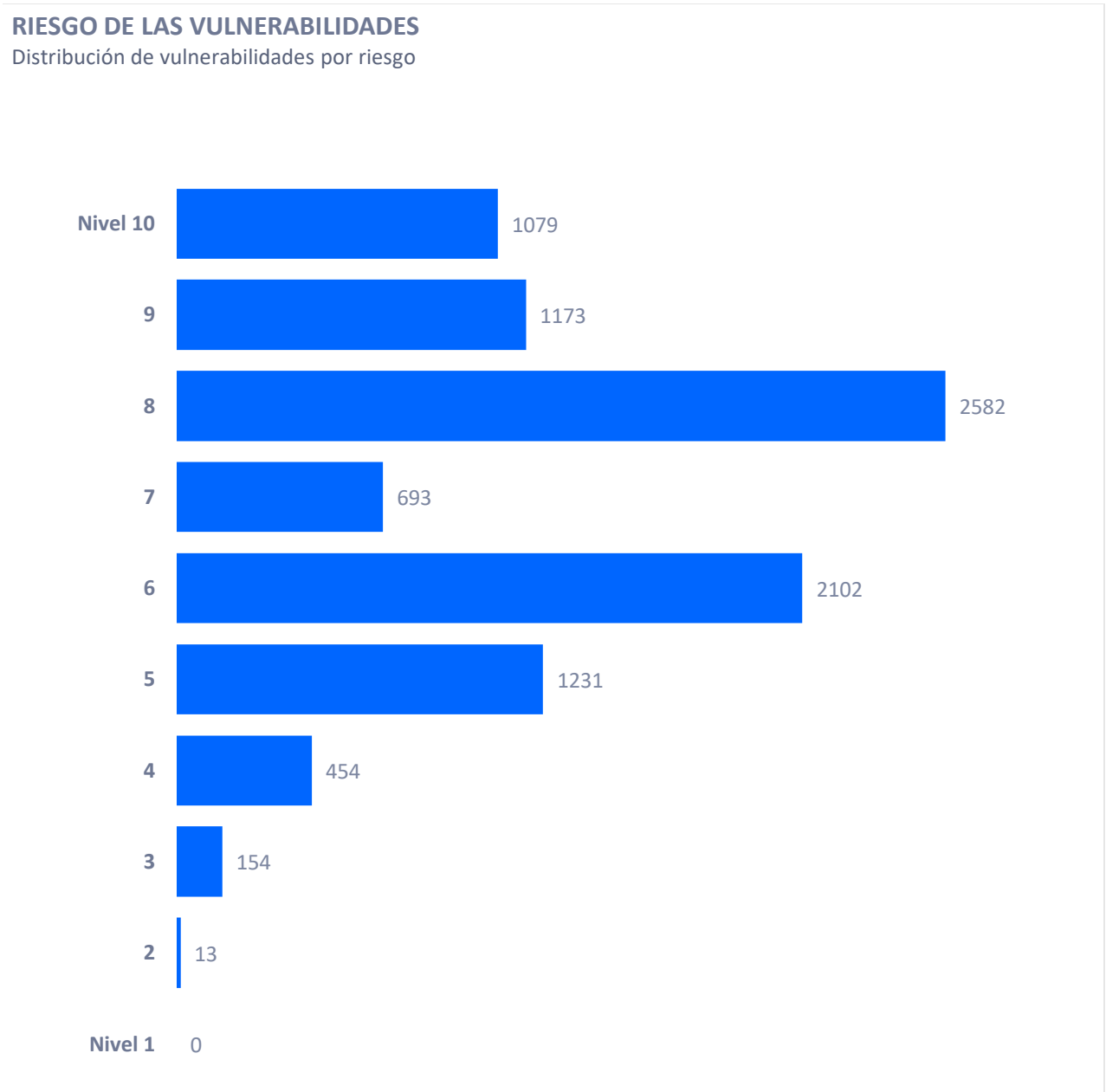
Comentamos en esta sección algunas de las vulnerabilidades notables a nuestro juicio, de este segundo semestre de 2021, es decir, aquellas que destacan por su especial relevancia o peligrosidad.

CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2021-34527, CVE-2021-1675 CVE-2021-36958	Windows Print Spooler	Varios fallos que permitían la elevación de privilegios como SYSTEM bajo ciertas circunstancias. Apodados #printNightmare son un conjunto de fallos que se encontraron durante la segunda mitad del año.	8.8
CVE-202121166 CVE-2021-30551	Google Chrome	Ejecución remota de código en Chrome y escapada de la sandbox. Usadas por un atacante (0day) y descubiertas por el Threat Analysis group del propio Google.	8.8
CVE-2021-33909	Elevación de privilegios en el kernel de Linux	Apodada Sequoia y encontrada por Qualys, explotaba el sistema de ficheros.	5.5
CVE-2021-28139 y otros tantos	Bluetooth	Hasta 16 fallos se encontraron en la implementación de BlueTooth de ESP32 SoC, que es muy sado en la industria. La más grave permitiría ejecución de código.	8.8
CVE-2021-42574 y CVE-2021-42694	Trojan Source Attacks	Ataque que conseguían introducir codificaciones no habituales en los comentarios de los códigos fuentes y el compilador podría llegar a modificar el comportamiento del código, aunque no quedase visible para el humano en el código fuente.	8.3
CVE-2021-23849	IP-CAM Bosch hasta CPP14, versión 8.00 y AVIOTEC, versiones 7.61 y 7.72	Vulnerabilidad en cámaras IP de seguridad de Bosch, que permite que un atacante ejecute acciones y cambie parámetros en éstas haciendo uso de CSRF.	7.5
CVE-2021-24672	SoftControl 800xA 6.1.	Vulnerabilidad en la herramienta Softcontroller, de ABB. Esta herramienta, implementada para pruebas y debug de programación en los dispositivos, permite el acceso remoto y la modificación y ejecución de código.	9.8

CVE-2021-28139	BrakTooth	vulnerabilidad perteneciente al grupo BrakTooth, afecta a los procesadores ESP32, de amplia utilización en dispositivos IoT relacionados con el ámbito industrial. La explotación de esta vulnerabilidad podría tener graves consecuencias incluso en la seguridad de las personas y de las infraestructuras críticas, ya que permite, entre otras, tomar el control de las comunicaciones, bloquear los dispositivos por completo…	8.8
CVE-2021-44228 CVE-2021-45046 CVE-2021-4104	Log4shell	Varios fabricantes de dispositivos del ámbito industrial hicieron pública la afectación de sus dispositivos al 0-day conocido como “Log4shell”. El impacto es profundo y variado, pero con un potencial muy grave. La lista completa se puede consultar en: https://www.incibe-cert.es/alerta-temprana/avisos-sci/vulnerabilidad-log4shell-afecta-sistemas-control-industrial	10

Las vulnerabilidades en cifras

En números concretos de vulnerabilidades descubiertas, la distribución de CVE publicados por nivel de riesgo (*scoring* basado en CVSSv3), ha sido la siguiente:

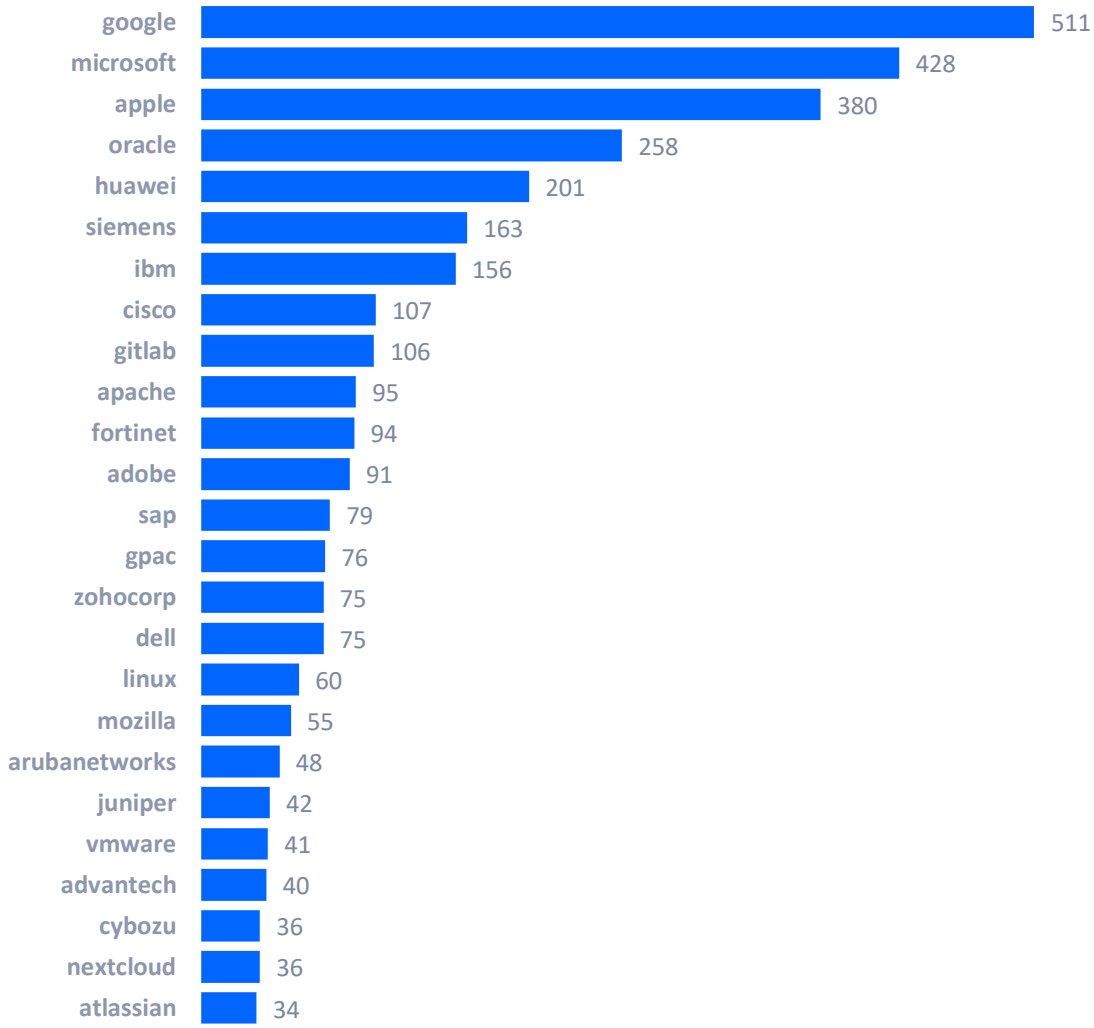


Top 25 compañías con más CVE acumulados

Durante el segundo semestre de 2021, Google ha liderado por número de vulnerabilidades conocidas.

VULNERABILIDADES POR FABRICANTE

Top 25 fabricantes por CVE acumulados



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.**

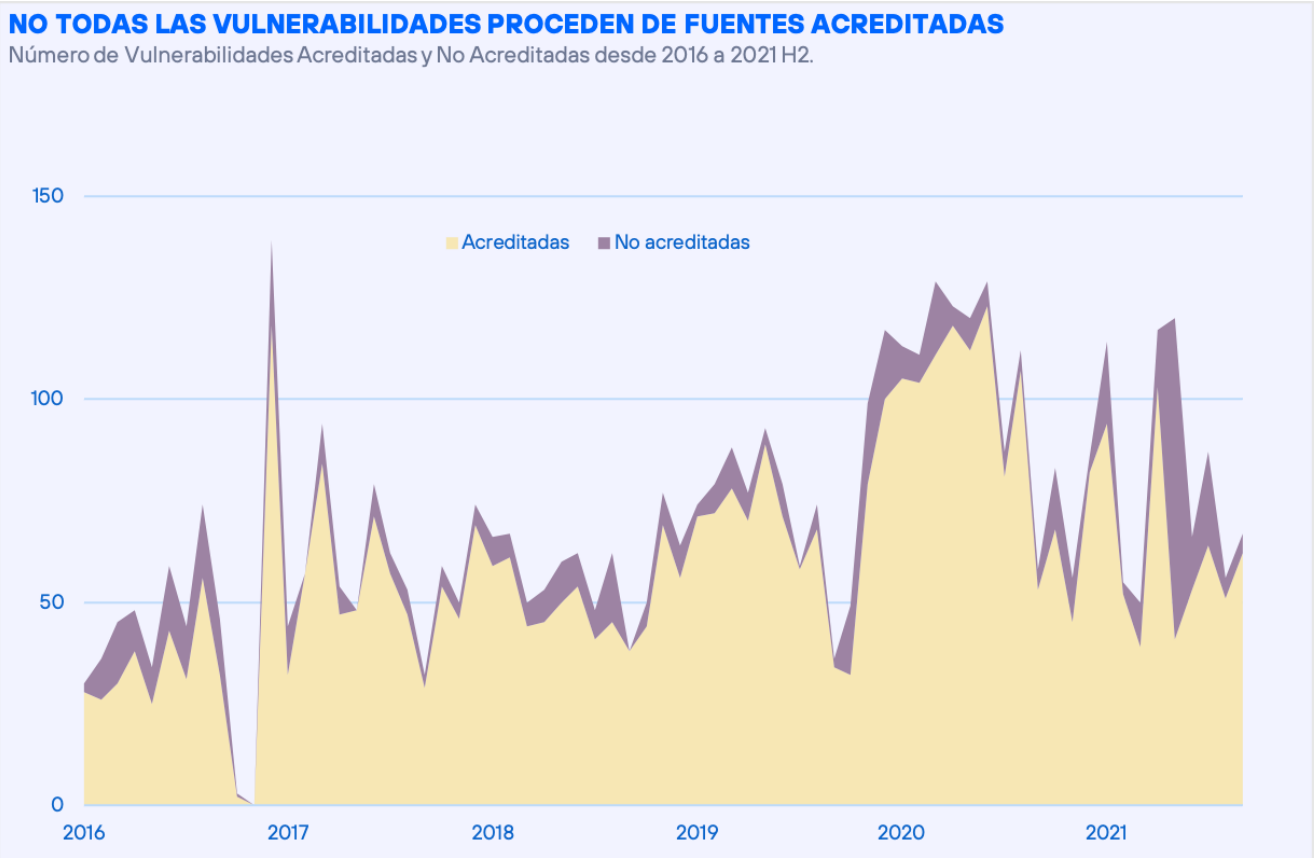
Metodología

Hemos realizado algo muy simple. Hemos recopilado y procesado toda la información de CVEs acreditadas durante el segundo semestre de 2022. 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 384 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 500). 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:



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.

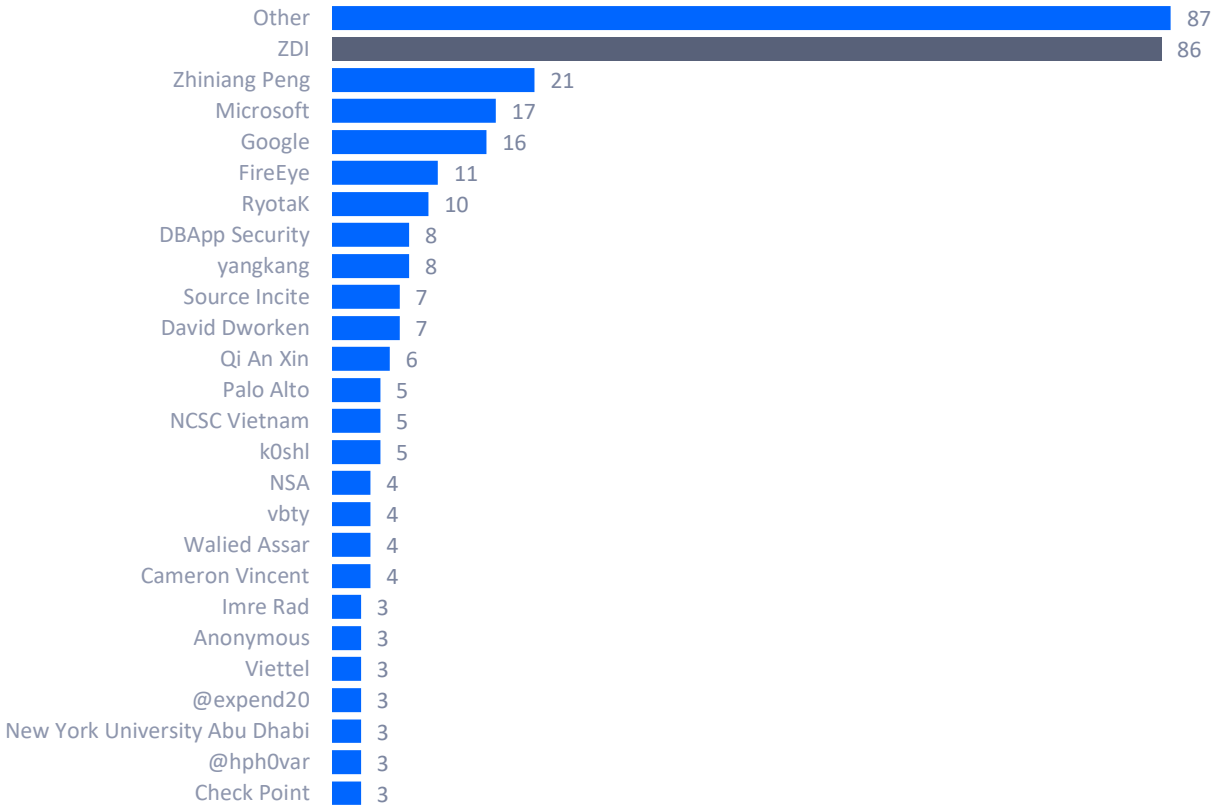
A partir de ahí, hemos realizado diferentes cálculos para poder analizar quién contribuye más y mejor a mejorar la seguridad de los productos Microsoft, de manera responsable.

Los datos

Comparados con el semestre anterior, los datos resultan muy diferentes. La larga cola de “otros” es la que lidera la lista. Esto quiere decir que son descubiertas por investigadores con menos de 5 fallos acumulados. La iniciativa ZDI, sigue siendo (cada vez más) la fórmula favorita para los investigadores. Se cuela de nuevo este trimestre Zhiniang Peng como un actor muy relevante con 21 fallos.

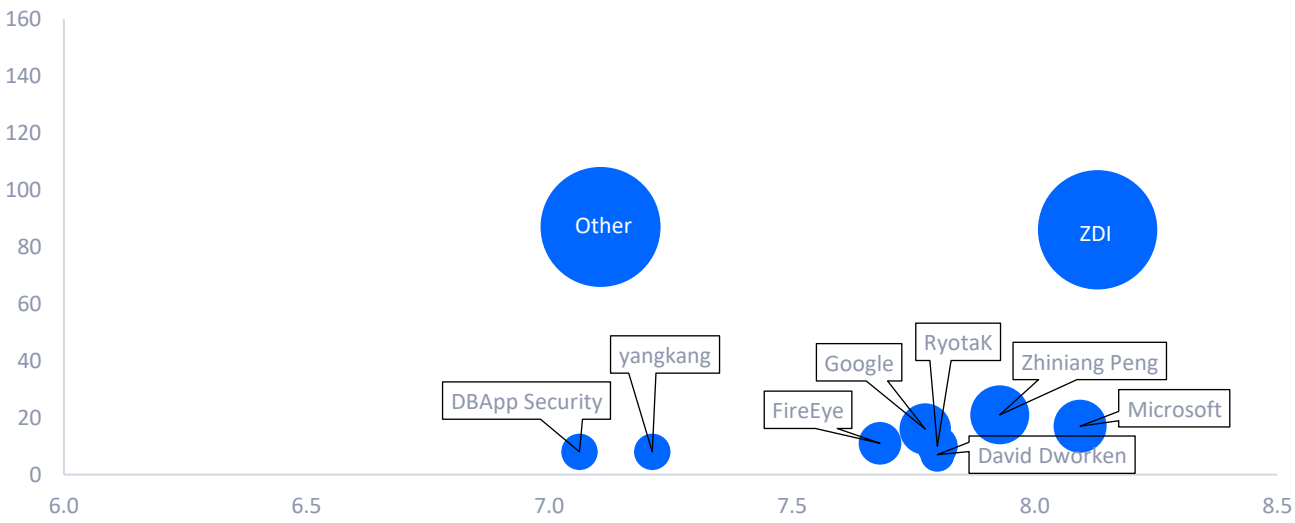
ZDI ES EL GRUPO QUE MÁS VULNERABILIDADES DESCUBRE EN PRODUCTOS DE MICROSOFT

Número total de vulnerabilidades por cada descubridor en el segundo semestre de 2021



ZDI TAMBIÉN DESCUBRE LOS FALLOS MÁS GRAVES

Distribución de vulnerabilidades por gravedad y por descubridor; el tamaño de la burbuja es proporcional al número de vulnerabilidades descubiertas durante 2021 H1.



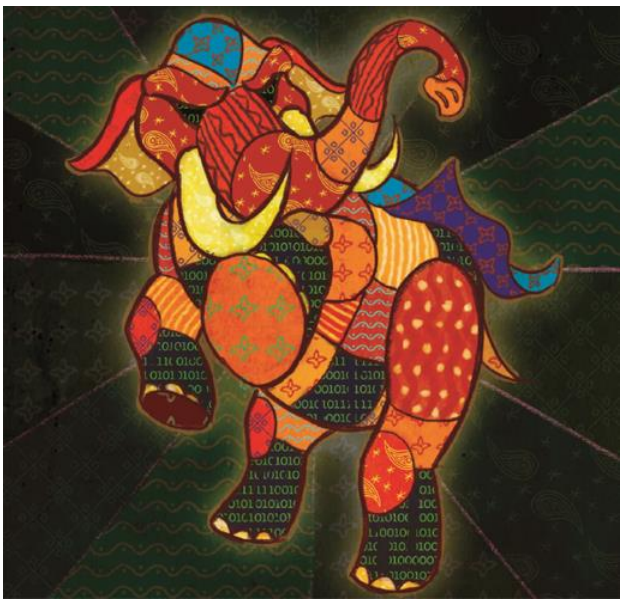
OPERACIONES APT, GRUPOS ORGANIZADOS Y MALWARE ASOCIADO

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 2022



Patchwork: ¿obra de arte o amalgama de sobras?

Recientemente, los investigadores de Malwarebytes publicaron un análisis de este APT group de origen indio, activo desde 2015, que comenzó a finales de noviembre una campaña contra entidades y organismos públicos pakistaníes, como el Ministerio de defensa y el ICCBS, entre otros. Toda la información que recopilaron estos investigadores se la facilitó el propio APT-Group, porque se infectó con su propio malware. Un interesante giro del destino.

¿Y por qué se le llama Patchwork a este grupo? Patchwork es una técnica de costura que consiste en crear prendas de tela (colchas, vestidos, trajes, lo que sea) utilizando sobrantes, o retales de tela. Este grupo hace algo similar. No en vano, el desaparecido grupo israelí de investigación "Cymmetria" los llamó "The copy-paste APT", ya que su principal TTP era copiar código de foros y repositorios para componer sus armas y herramientas.

El dibujo del APT-Group que figura arriba se encuentra en la portada de su estupendo informe, de 2016, en el que analizaban a este grupo. Via InternetArchive .

Más información en https://thehackernews.com/2022/01/badnews-patchwork-apt-hackers-score-own.html

Primitive Bear (AKA Gamaredon): Unmasked

En noviembre, algunos de los presuntos miembros de este grupo ruso, uno de los APT-Group más activos contra Ucrania, fueron identificados. Según los investigadores, se trata de ucranianos que en estos momentos son agentes del FSB (y, por lo tanto, tratados como traidores a su país).

El grupo está asociado con más de 5.000 ciberataques contra 1.500 sistemas gubernamentales ucranianos.

Más información en: https://therecord.media/ukraine-discloses-identity-of-gamaredon-members-links-it-to-russias-fsb/

Acuatic Panda: De la piscina a la universidad

No sabemos si nadan, pero sabemos que les gustan las piscinas. Y después de relajarse en la piscina, a la universidad. Pero no a estudiar, sino a robar información de inteligencia y espionaje industrial. Eso indican los investigadores de CrowdStrike, que los han pillado explotando la ya famosa “Log4Shell” en una institución académica (eso es lo único que confirman) no revelada. Al fin y al cabo, la colaboración con grupos de investigación de grandes universidades es habitual en ciertos casos, y pese a trabajar en proyectos delicados, suelen tener medidas de seguridad potencialmente menores que las que tendrían grandes empresas o redes militares.

Más información en: https://threatpost.com/aquatic-panda-log4shell-exploit-tools/177312/

ANÁLISIS DE AMENAZAS OT

La siguiente información procede del sistema para la captura y análisis de amenazas en el ámbito OT, Aristeo. **Aristeo** incorpora una red de **señuelos, fabricados con hardware industrial real,** que aparentan ser sistemas industriales en producción real, **y se comportan como tales**, pero que están extrayendo toda la información sobre las amenazas que acceden al sistema. Con la información de todos los dispositivos desplegados en los distintos nodos-señuelos, Aristeo aplica relaciones e inteligencia para ir más allá del dato, pudiendo detectar proactivamente campañas, ataques dirigidos o sectorizados, vulnerabilidades 0-day, etc.

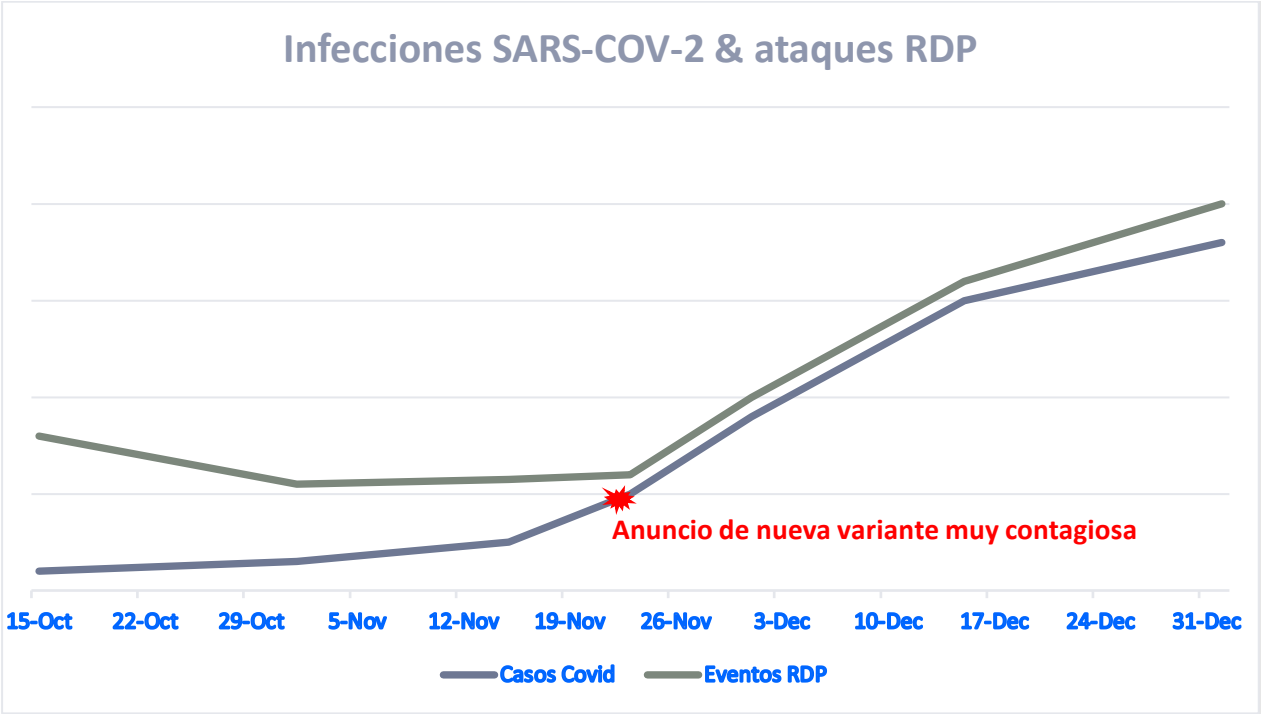
Cada nodo-señuelo dispone de sus propias características y reproduce un proceso distinto. Por lo tanto, los protocolos, dispositivos, sectores productivos... cambian en cada uno de ellos. Además, los nodos están vivos, lo que implica que pueden experimentar alteraciones en su configuración a gusto del equipo de investigadores que trabajan con ellos, o del cliente que dispone de su uso temporal o permanente. Esta variabilidad puede generar ligeras discrepancias en los datos mostrados en este apartado si se comparan entre semestres.

Más información en:

https://aristeo.elevenlabs.tech

Análisis de la información

Si el primer trimestre inauguramos la sección con la temática Ciberseguridad & COVID-19 por ser el tema de los primeros seis meses de 2021, el segundo semestre no fue (desgraciadamente) muy distinto. De hecho, en una de nuestras revisiones periódicas de los datos, nos dimos cuenta de que la tendencia del semestre anterior parecía cumplirse de nuevo. De hecho, hasta octubre, el aumento de las interacciones contra los PLC había aumentado, llegando a ser dominante en todo octubre y los inicios de noviembre… hasta que llegó una variante nueva del virus que iba a entrar con fuerza en todo el mundo .Y se volvió a cumplir eso que dijimos en el otro informe de “siempre se ha comentado que los delincuentes son los que mejor conocen la sociedad y sus realidades, su legislación...”.



La gráfica lo deja claro, puesto que es su sustento y su supervivencia depende de ello.

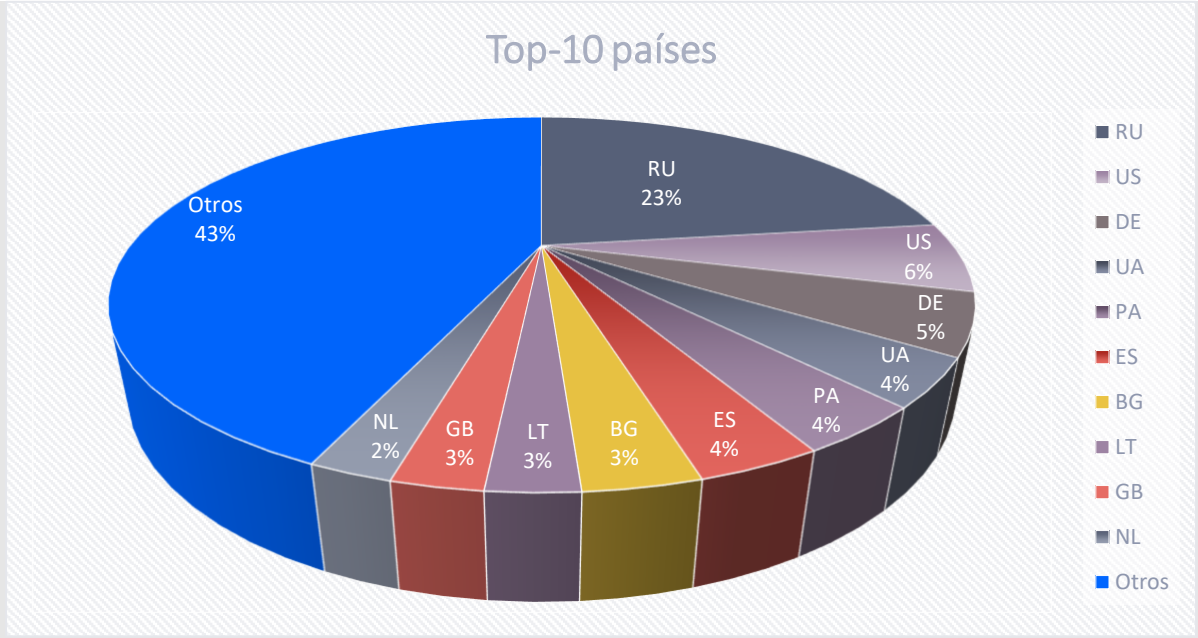
Igual que en el semestre anterior, los datos de las amenazas cibernéticas provienen en su totalidad de nuestro sistema, mientras que los datos de infecciones con SARS-COV-2 provienen de varios gobiernos y entidades investigadoras de reconocido prestigio. Aun así, dado que se han aglutinado datos de España, Francia, Alemania, Italia y Reino Unido, la actualización y trazabilidad de esta información no siempre es la mejor.

Una vez señalado esto, vamos a ver la tendencia. La gráfica vuelve a mostrar la misma que el semestre anterior. Se aprecia como los ataques sobre RDP habían disminuido hasta alcanzar un valor mínimo donde se mantenían estables, a la vez que otros sí aumentaban. Mientras tanto, los casos de COVID-19 seguían al alza y sin cambios en su tendencia, porque al virus le da igual si declaramos sus mutaciones dignas de estudio o no. Sin embargo, en cuanto la noticia saltó al mundo entero, los intentos de acceso remoto cambiaron radicalmente de tendencia y volvieron a ser dominantes… y lo siguen siendo mientras redactamos estas líneas.

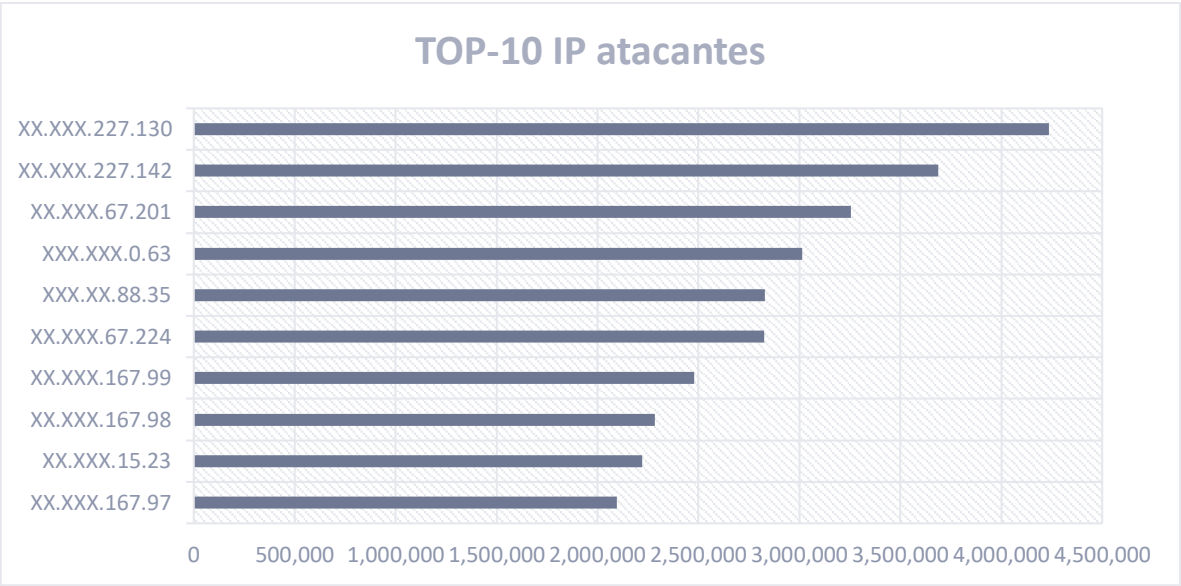
Pasamos a la estadística genérica de la información registrada. En el segundo semestre de 2021 se detectaron más de 402 millones de eventos de ciberseguridad. Esto supone un incremento de más del 160% respecto a los registrados en el primer semestre de 2021.

Mayoritariamente, los eventos han estado relacionados con ataques de RDP más o menos sofisticados, pero hemos tenido un último trimestre de lo más interesante, con ataques centrados en los PLC. Concretamente, en el mes de octubre el aumento fue del 1500% (tal cual). Sólo uno de los PLC recibió más de 4.5 millones de interacciones.

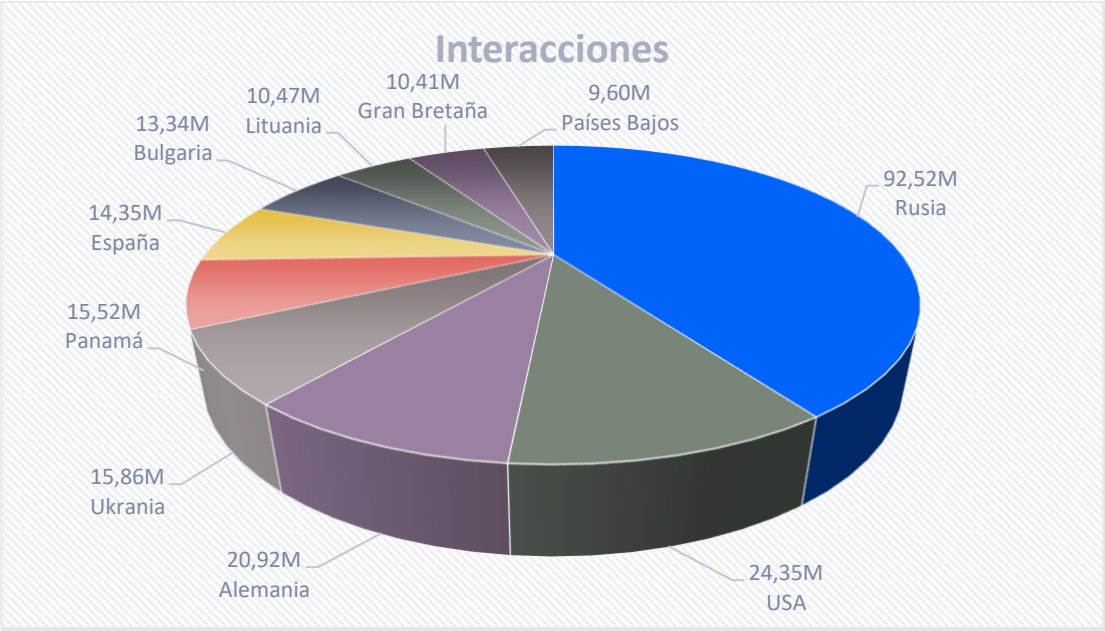
La distribución por países sería la siguiente:



Ahora vamos a ver el Top-10 de las direcciones IP con más interacción con el sistema de Aristeo. Del TOP-10, el 40% pertenecen al mismo proveedor de servicios de un país (del que ya hablamos en el informe anterior).



A continuación, observamos cómo se reparten las IP con más actividad. Como dato curioso este mes, podemos constatar que las dos direcciones con más actividad pertenecen al mismo país y representan más del 50% de las interacciones que ha tenido ese país con nuestro sistema.



RECAPITULACIÓN

En el ámbito de la seguridad para móviles, el número de vulnerabilidades en **IoS es menor que en 2020, pero las que existen, son más graves.**

Con respecto al informe de transparencia de Apple, el gobierno alemán es el que más solicitudes ha generado para obtener información sobre dispositivos. Mientras que, como de costumbre, China es el país que más retirada de apps solicita en el App Store.

Respecto a las vulnerabilidades y debilidades, en la segunda parte de 2021 se ha observado un cambio interesante: **Los tres fabricantes con más CVE asociados no siguen siendo los mismos: Microsoft, Google y Oracle, sino que este último se ve sustituido por Apple.**

Respecto a la actividad de los grupos APT, se observa un incremento de actividad en los últimos meses. Con respecto al análisis de amenazas OT, hemos podido comprobar que es cierto eso que se dice sobre que los delincuentes son los que mejor conocen la legislación y la realidad de la sociedad. Además, observamos la realidad de estos entornos: aunque parezca que permanecen en un segundo plano, no es cierto. En cuanto apareció la variante ómicron, se dispararon ciertos tipos de ataques relacionados con el teletrabajo.

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 ciberseguridad de Telefónica Tech tenemos mucha más información y noticias que pueden resultar de tu interés. Aquí van nuestros artículos más relevantes.

IDENTIDAD

¿Son seguros los SMS para el envío de códigos de verificación?

Crónica del ataque a un youtuber que sabía de ciberseguridad

CRIPTOGRAFÍA

Panorama de los certificados SSL en España

MALWARE

Snip3, una investigación sobre malware

¿Qué contiene el "curso en ciberseguridad" que deben seguir los atacantes afiliados de Conti, el ransomware de éxito?

¿Por dónde ataca el ransomware? Tres pilares fundamentales

Análisis del código fuente del ransomware Babuk: Nas y esxi

INTELIGENCIA ARTIFICIAL

Informe de convergencia entre IoT, Big Data e IA