Telefónica Tech

Informe sobre el estado de la seguridad 2024 H1

Desde la seguridad en móviles hasta el análisis de vulnerabilidades, desde las noticias más relevantes hasta el seguimiento de amenazas, 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.

Comienza 2024 con noticias muy relevantes en el mundo de la ciberseguridad, aunque esto ya se ha convertido en la norma. El semestre anterior destacábamos que Chrome sufrió 8 vulnerabilidades 0day en todo 2023 y, en lo que llevamos de 2024, ya se ha alcanzado esa cifra. Sin duda, el "monocultivo" que supone el motor Chromium ha motivado a los atacantes a aprovechar los fallos en este software. El listón de seguridad se eleva tanto como la habilidad de los atacantes.

En esta línea, destacamos el ataque a Microsoft por parte de Midnight Blizzard, que robó información de Microsoft en el ataque de enero y usaron los datos para obtener acceso no autorizado a repositorios y otros sistemas internos. La historia se repite. En 2002 Microsoft lanzó una iniciativa llamada "Trustworthy Computing" que supuso un cambio de paradigma, priorizando un desarrollo seguro a nivel de toda la compañía y cambiando la visión, más o menos extendida, entre los usuarios de que Microsoft de que su software contenía muchos fallos y problemas de diseño que lo hacían inestable. A finales de 2023 Microsoft se ha vuelto a ver obligado a realizar una comunicación similar a través de CEO Satya Nadella tras una serie de incidentes de alto perfil que de nuevo han afectado a la reputación de Microsoft y cuestionado su cultura y postura de seguridad por parte de muchos expertos de ciberseguridad a nivel global. La nueva Secure Future Iniciative intenta funcionar con la seguridad por diseño, por defecto y realizar operaciones seguras. Veremos los frutos de esta iniciativa a lo largo de los siguientes años.

Y es que los atacantes nos están poniendo a prueba. La enorme sofisticación del ataque a Linux a través de la librería XZ que ocurrió en este primer semestre, deja a las claras la complejidad que están consiguiendo los ataques. No solo en el plano técnico, no solo en la cadena de suministro... Este ataque demuestra la importancia y el impacto de la confianza, como nuevo vector de ataque. Haberse ganado la confianza de un desarrollador, colaborar de forma activa con un proyecto durante años, todo para, en el momento adecuado, modificar el código de forma tan inteligente como para que pase desapercibido y solo se distribuya en paquetes para evitar ser visto en los repositorios... Una estrategia impecablemente paciente desde el punto del atacante, pero que nos obliga a replantear incluso el modelo de colaboración y reputacional en software libre.

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 2024

A continuación, damos cuenta de aquellas noticias que mayor impacto han tenido durante el transcurso de este primer semestre de 2024.

ENERO

- **Midnight-blizzard ataca Microsoft**: Los atacantes, presuntamente patrocinados por el estado ruso, han violado la red interna de Microsoft y han robado correos electrónicos del equipo de liderazgo, legal y de ciberseguridad de la compañía. **La intrusión comenzó a finales de noviembre de 2023 y duró hasta el 13 de enero**.
- **Ivanti connect secure:** El 10 de enero, Ivanti publicó un aviso de seguridad sobre dos vulnerabilidades en su dispositivo VPN Connect Secure (anteriormente Pulse Secure) que estaban siendo explotadas activamente. Estos dos zero-days se identificaron como CVE-2023-46805 (bypass de autenticación) y CVE-2024-21887 (inyección de comandos). **El aviso de seguridad de Ivanti no incluía parches de firmware, sino solo mitigaciones temporales** en forma de un archivo XML cifrado que los clientes debían ejecutar en sus dispositivos. Se estima el impacto en **más de 1.700 aplicativos infectados durante las primeras fases del ataque**.
- **Vulnerabilidad crítica en Gitlab:** GitLab publicó actualizaciones de seguridad para las ediciones Community y Enterprise con el fin de solucionar dos vulnerabilidades críticas (CVE-2023-7028, CVE-2023-5356), una de las cuales permite el **secuestro de cuentas sin interacción del usuario**.
- **23-and-me:** La compañía **intentó culpar a sus usuarios por su violación de datos en enero, alegando que son responsables por usar contraseñas débiles**. La compañía fue demandada más de 30 veces por su reciente violación de seguridad y después de que la compañía **modificara de forma unilateral sus términos de servicio para forzar a la gente a entrar en arbitraje**.
- **Scraping para modelos IA:** El organismo de vigilancia de la privacidad del Reino Unido (ICO) lanzó un análisis de la legalidad de las empresas de IA que extraen contenido web para entrenar modelos generativos. **La iniciativa analiza si la práctica infringe las leyes de propiedad o de contrato y su cumplimiento con las leyes de protección de datos existentes.**
- **Schneider Electric afectado por el ransomware "Cactus":** Según BleepingComputer, el ataque, efectuado el 17 de enero, afectó a la división de negocios de sostenibilidad de la compañía. Esta área ofrece servicios de consultoría a empresas, centrándose en el negocio de energías renovables. Según el medio, los atacantes robaron "terabytes" de datos, incluyendo información confidencial sobre la infraestructura industrial de los clientes de la empresa.

FEBRERO

- **KeyTrap (CVE-2023-50387):** Es probablemente "el peor ataque al DNS descubierto nunca". Una denegación de servicio en servidores DNSSec (hoy se usa en un 31% de las resoluciones) y precisamente por procesar claves criptográficas. La vulnerabilidad puede agotar los recursos de CPU en los servidores DNS y paralizar las búsquedas de nombres de dominio. La **explotación solo requiere un paquete malicioso**, **y algunos servidores DNS pueden quedar inactivos hasta 16 horas**. Microsoft, BIND, PowerDNS y la mayoría de las principales distribuciones de Linux han lanzado parches para KeyTrap.
- **Desmantelada infra de LockBit:** La Agencia Nacional contra el Crimen del Reino Unido (NCA), en colaboración con agencias policiales de otros 10 países entre las que se encuentra el FBI, **han interrumpido la infraestructura y servicios de los operadores del ransomware LockBit**. Los hechos tuvieron lugar el lunes 19 de febrero, según Cyberscoop, el FBI ha obtenido acceso a casi 1.000 claves de descifrado, lo que permitiría la posible recuperación o remediación de las operaciones de extorsión de LockBit que se encuentran en curso. Los gestores de LockBit han identificado que habrían sido comprometidos debido a la explotación de la vulnerabilidad de PHP registrada como CVE-2023-3824.
- **Ransomware Rhysida descifrado:** Investigadores surcoreanos han roto el esquema de cifrado utilizado por el ransomware Rhysida y han lanzado un descifrador que permite a las víctimas recuperar archivos sin pagar el rescate. L**anzar cualquier tipo de herramienta de descifrado que explote una vulnerabilidad en los binarios del ransomware constituye un dilema**. Esto se debe a que las bandas de ransomware simplemente arreglarán su código y eliminarán una forma de que las víctimas recuperen archivos.
- **Novedosa técnica de fingerprinting en Spyware:** ENEA, una empresa de seguridad de telecomunicaciones con sede en Suecia, afirma que ha reproducido un hackeo previamente desconocido. Entre la documentación del caso judicial entre Whatsapp y el Grupo NSO, se usaba el término "**MMS fingerprinting**". Este término es nuevo en la industria y no estaba presente en internet excepto en un caso judicial. **El ataque revela el dispositivo objetivo y la versión del sistema operativo a través de un MMS enviado al dispositivo sin interacción, participación o apertura de mensajes por parte del usuario**.
- **Controvertido acuerdo entre Reddit y Google:** Reddit y Google han cerrado un acuerdo de **60 millones de dólares que permite a Google Entrenar Modelos de IA con las publicaciones de Reddit**. Además, Google también proporcionará a Reddit herramientas para mejorar su búsqueda interna**.**
- **Ataque cibernético a Varta:** El conocido fabricante de baterías Varta se vio obligado a **cerrar la producción en cinco fábricas como consecuencia de un ataque cibernético**. El incidente tuvo lugar el 12 de febrero, y también afectó a la red administrativa de la empresa. La compañía dice que desconectó las redes afectadas de internet mientras investigaba el incidente.
- Más de 100 hospitales rumanos se ven afectados por un Ransomware: Durante el fin de semana del 10 al 11 de febrero, un atacante llegó hasta el sistema de información "Hipocrate", ampliamente utilizado, y cifró datos pertenecientes a 26 hospitales en todo el país con el ransomware Backmydata. El primer afectado fue un hospital infantil el 10 de febrero. Otras 74 instalaciones médicas conectadas a este sistema fueron aisladas para ser analizadas y aseguradas.

MARZO

- **Parche de seguridad crítico de VMWare:** VMware se ha visto obligada a parchear un conjunto de vulnerabilidades **incluso en versiones de productos afectados que ya no tenían soporte**. La razón es la gravedad de los fallos descubiertos, algunos de ellos con un 9.3 de 10 en la escala del estándar CVSS. **Los fallos están relacionados con el controlador USB que permite a las máquinas virtuales acceder al hardware del huésped como si éste estuviera conectado directamente al sistema virtualizado**.
- **Atasco en el enriquecimiento del NVD del NIST:** La NVD (National Vulnerability Database) del NIST publicó el 15 de febrero un anuncio de que está estableciendo un consorcio para abordar los desafíos de recursos dentro de la organización. Tras ese anuncio durante las posteriores semanas El NIST solamente **enriqueció 59 entradas de CVE, dejando más de 2.100 vulnerabilidades sin ninguna descripción o contexto**. **El impacto es considerable en la comunidad de la seguridad, ya que el NIST es el principal editor y enriquecedor de CVEs y por tanto una parte central de muchos sistemas de seguridad actuales**.
- **Ley de IA de la UE:** El Parlamento Europeo aprobó en marzo la Ley de Inteligencia Artificial, el primer gran acto del mundo para regular el uso de la IA. La ley fue aprobada con 523 de 618 votos. La nueva legislación **prohíbe el uso de aplicaciones de IA que amenacen los derechos de los ciudadanos**. **Esto incluye la categorización biométrica, el reconocimiento de emociones y los sistemas de policía predictiva**. La Ley de IA de la UE incluye exenciones, para el uso de sistemas de identificación biométrica por parte de las agencias de aplicación de la ley, bajo condiciones estrictas.
- **Trello – Correos electrónicos de 15 millones de usuarios en venta:** Un actor, con el seudónimo de emo, puso a la venta en un conocido foro de hacking, datos de 15 millones de usuarios de Trello con información pública y privada de los mismos: nombre de usuario, nombres completos y correos electrónicos asociados.
- **AWS – Ataque de denegación de cartera**: Un nuevo método de ataque en AWS permite a los atacantes crear una gran cantidad de solicitudes *RANGE* para partes de archivos grandes (>1GB) antes de cancelar rápidamente la solicitud. **Esto factura a los propietarios por la solicitud completa, lo que puede resultar en una amplificación de costes de hasta 50 veces**.
- **Los robos a criptomonedas continúan su goteo continuo:** como ejemplo, durante el mes de marzo, un atacante ha **robado criptoactivos por valor de 6,5 millones de dólares de la plataforma de comercio de criptomonedas Seneca**. La compañía confirmó y atribuyó el ataque a una vulnerabilidad en sus contratos inteligentes. Seneca recuperó el 80% de los fondos robados después de permitir que el atacante se quedara con el 20% como un "esfuerzo de *hacking de sombrero blanco*", sea lo que sea que sea que eso signifique**.**
- Investigadores del Instituto de Tecnologías de Georgia (Atlanta) publicaron un estudio en el que se analizan las posibilidades de ejecutar ataques remotos similares a los del malware Stuxnet contra sistemas actuales. Para demostrar su teoría, los investigadores desarrollaron un malware diseñado para aprovechar los sitios web de los PLC como vector de entrada. Tras acceder, el malware intenta abusar de las API web de los PLC para interrumpir los procesos en ejecución o modificarlos, causando daños al hardware.

ABRIL

- **Vulnerabilidad crítica hallada en XZ:** Se detectó una vulnerabilidad crítica CVE-2024-3094, **CVSSv3 10 sobre 10**, en las versiones 5.6.0 y 5.6.1 de la utilidad de compresión XZ y sus bibliotecas *liblzma* asociadas. El código malicioso, no presente en los repositorios Git públicos pero alojado en los *tarballs* de las *releases* oficiales, fue insertado intencionalmente por un contribuidor del proyecto y **representa una amenaza significativa contra sistemas Linux al manipular procesos de autenticación elementales empleados**. Todo apunta a la preparación de un ataque masivo a la cadena de suministro.
- **Sandbox V8 de Chromium:** Tras tres años de espera, ya está aquí la *sandbox* de V8, el motor JavaScript de Chromium o lo que es lo mismo, el de casi todos los navegadores menos Firefox. Esto es muy relevante porque permite extender la *sandbox* a un lugar todavía vulnerable del navegador. De hecho, entre 2021 y 2023, el 60% de las vulnerabilidades en Chrome que acabaron en explotación y ejecución de código se produjeron por corrupción de memoria en V8.
- **Distribución de malware**: Ciberdelincuentes están utilizando **comentarios en incidencias de GitHub para alojar archivos maliciosos en los repositorios oficiales de empresas legítimas**. El ataque consiste en crear una incidencia en un proyecto oficial y subir el archivo malicioso como un comentario, pero no reportar la incidencia. La incidencia nunca está activa o visible para el propietario del proyecto. **La URL del archivo engañará a los usuarios haciéndoles pensar que es un archivo oficial de ese proyecto**, incluso si fue subido por un atacante.
- **Modo incógnito de Chrome:** Google llegó a un acuerdo en una demanda colectiva y ha acordado eliminar los datos de usuario que recopiló a través del modo de navegación privada del navegador Chrome. **La compañía fue demandada por violar la privacidad del usuario en 2020,** después de que los usuarios descubrieran que Google estaba rastreando sus movimientos incluso en sesiones de navegación privada de Chrome. **Google llegó a un acuerdo en la demanda después de que los demandantes supuestamente pidieran 5 mil millones de dólares en daños**. Como parte del acuerdo, Google también rediseñará el modo de navegación privada de Chrome.
- **Incidente Deepfake en LastPass:** Un actor de amenazas utilizó una grabación *deepfake* de su CEO en un intento de engañar a uno de sus empleados. El empleado no cayó en **la estafa porque la solicitud llegó a través de WhatsApp, un canal de negocios poco común**.
- La tecnología Voice Engine de OpenAI, capaz de clonar voces con solo 15 segundos de audio, ha sido considerada demasiado arriesgada para una liberación generalizada debido a preocupaciones de desinformación y también que el **Reino Unido se ha comprometido a introducir leyes que hacen que la creación de *deepfakes* explícitos sin consentimiento sea un delito**.
- **Fallo criptográfico en PuTTY**: Un equipo de académicos alemanes ha descubierto una vulnerabilidad criptográfica en PuTTY, un cliente SSH y Telnet extremadamente popular para usuarios de Windows. La vulnerabilidad permite a los atacantes observar firmas criptográficas y recuperar la clave privada de un usuario. El **principal impacto de la vulnerabilidad está en los repositorios de código fuente si han sido gestionados a través de un cliente que integra PuTTY**. Los atacantes pueden mirar las firmas públicas pasadas de un proyecto y luego determinar la clave privada de un desarrollador, esto **abre la puerta a ataques a la cadena de suministro donde los actores de amenazas pueden enviar código malicioso "firmado" a proyectos legítimos**.

- CISA emitió el 11 de abril una directiva de emergencia en la que solicitaba que se buscaran señales (IoC) de compromiso del APT Group "Midnight Blizzard", quien consiguió llegar a la red corporativa de Microsoft y accedió a correspondencia de varias agencias gubernamentales de los Estados Unidos.

MAYO

- **Microsoft Secure Future Iniciative**: Tras los incidentes relacionados con *Midnight Blizzard* a principios de año, Microsoft, en un artículo publicado este mes de mayo, detalla la aceleración y extensión del SFI (Secure Future Iniciative) dentro de la compañía tras las recomendaciones recibidas por el comité de ciberseguridad del departamento de estado americano. Un detalle importante es que Microsoft está dispuesto a hacer una fuerte apuesta por asegurar su correcta ejecución a través de una **modulación de la compensación del liderazgo de Microsoft en función de los avances e hitos del plan SFI**. Un redoble de tambores en toda regla.
- **Malware en Android**: El malware no deja de llegar a Google Play. Se **encontraron 90 apps que habían conseguido instalarse en 5.5 millones de Androids**. Todas derivaban en la infección con Anatsa (o Teabot), un troyano bancario para Android que puede robar información de 650 bancos de todo el mundo. Desde finales de 2023, esta campaña ha llegado a 150.000 apps de Google Play. **Además, casi todas disfrazadas bajo la modalidad de "productividad"**.
- **Ataque masivo a plugin de Wordpress**: Se divulgó una vulnerabilidad de severidad 9.9 en el plugin WordPress Automatic. La vulnerabilidad es una inyección SQL que podría permitir a atacantes no autenticados crear cuentas de administrador y tomar control de un sitio de WordPress. *WPScan* ha registrado más de 5 millones de intentos de explotar la vulnerabilidad desde su divulgación.
- **Ticketmaster se enfrenta a una demanda colectiva por una masiva violación de datos:** *Live Nation Entertainment* reconoció una violación de datos en una presentación regulatoria después de que un individuo afirmara estar vendiendo datos de 560 millones de clientes de Ticketmaster en foros de hacking por 500.000 dólares. **Live Nation tardó 11 días en confirmar la masiva violación de datos de Ticketmaster**. La violación involucró el **acceso no autorizado a una base de datos en la nube de terceros que contenía datos de clientes como nombres, direcciones y detalles de tarjetas de crédito**.
- **Prohibir apostrofes para evitar inyecciones de SQL**: Un gobierno local del Reino Unido ha prohibido el uso de apóstrofes en los nombres de las calles de la ciudad para evitar problemas con sus sistemas informáticos. La mejor protección contra la inyección SQL que hemos escuchado.
- **Educación en ciberseguridad en la UE:** La agencia de ciberseguridad de la UE, ENISA, ha publicado una **guía** sobre cómo los estados miembros pueden evaluar la **madurez de su formación en ciberseguridad en los niveles de educación primaria y secundaria**. Más información.
- Rockwell emitió un aviso reiterando a sus clientes el consejo de desconectar de internet los dispositivos que no estén diseñados específicamente para la conectividad pública a internet. En su aviso citan explícitamente como razón "el aumento de las tensiones geopolíticas y la actividad cibernética adversa a nivel mundial."

- El FBI anunció el desmantelamiento de la mayor botnet a nivel mundial, "911 S5". La oficina estadounidense detuvo a su creador, un ciudadano chino de 35 años, que había llegado a infectar a más de 19 millones de dispositivos. Estos dispositivos fueron utilizados para cometer distintos delitos, entre los que se citan los de acoso, amenazas, fraudes y pornografía infantil. La operación fue coordinada por el DoD de los Estados Unidos y el FBI, pero en ella tomaron parte varias agencias de seguridad de todo el mundo.

JUNIO

- **Vulnerabilidad crítica en PHP para Windows**: El fallo de seguridad fue registrado como CVE-2024-4577, CVSSv3 de 9.8 según fabricante, y se debe a un fallo en el manejo de las conversiones de codificación de caracteres, específicamente la función "Best-Fit" en Windows cuando PHP se usa en modo CGI. La vulnerabilidad afecta a todas las versiones desde la 5.x y desde *Shadowserver* alertan tanto de que **actores maliciosos ya están comenzando a explotar el fallo de seguridad, como de que ya existe una PoC publicada**.
- **Ataques a usuarios VIP de TikTok**: Un ciberdelincuente parece estar utilizando un *exploit zero-day* para hackear y tomar control de cuentas de TikTok de alto perfil. El código malicioso se envía a las víctimas a través de mensajes directos de TikTok y **no requiere ninguna interacción del usuario excepto abrir el mensaje**. **Algunas de las cuentas hackeadas más grandes incluyen CNN, Sony y Paris Hilton**. TikTok anuncia que ya ha solucionado la vulnerabilidad zero-day que permitía a los atacantes tomar control de las cuentas, por tanto, es **muy recomendable asegurarse de actualizar a la última versión**.
- **Polémico cambio en los Términos de Servicio (ToS) de Adobe Photoshop:** Adobe estuvo bloqueando el acceso a su aplicación Photoshop a menos que los usuarios **acepten nuevos términos de servicio que otorgan a la compañía acceso completo a su contenido, el derecho a usarlo libremente e incluso sublicenciarlo a otros.** Después de la ola de críticas recibidas, de algunos de los creadores más importantes del mundo, **la compañía ahora está implementando un nuevo ToS que aclara específicamente que no utilizará ningún dato de cliente para entrenar su IA**.
- **Fuga de información del New York Times y su famoso juego *Wordle*:** Un atacante publicó un archivo de código fuente y datos robados pertenecientes al New York Times en *4chan*. **El filtrador afirma haber accedido al código fuente a través de un token de GitHub comprometido**, lo cual fue confirmado por el medio de comunicación. **Los datos filtrados supuestamente incluyen el código fuente del sitio web público de la compañía, aplicaciones móviles e incluso su juego Wordle**, la filtración contiene 270 GB de datos, la mayoría sin cifrar.
- **Función *recall* de Microsoft:** Investigadores de seguridad han demostrado cómo los ciberdelincuentes podrían robar datos recopilados por la función Recall de Microsoft. **Recall, activada por defecto en nuevos PC Copilot+, permite a los usuarios de Windows encontrar fácilmente información vista anteriormente en su PC mediante capturas de pantalla periódicas**. Tras la polémica generada **Microsoft ha cedido ante la presión pública y está implementando cambios en su función de Recall** de Windows 11. Dicha función se enviará **desactivada por defecto** para todos los sistemas compatibles con Windows 11.

- CISA ha notificado a los participantes del programa "CFATS" (Chemical Facility Anti-Terrorism Standards), que información entre la que se encuentra la información personal y cuentas de usuario, **podría haber sido comprometida tras el acceso ilegal a la "Herramienta de Evaluación de Seguridad Química" (CSAT).** Este acceso fue posible gracias a la explotación de una vulnerabilidad 0-day encontrada en un dispositivo Ivanti Connect Secure, en enero de 2024. El incidente podría afectar a más de 100.000 personas.

MÓVILES

Apple iOS

Las nuevas mejoras de seguridad de iOS 17

Como es tradición, las nuevas versiones de iOS se publican en el segundo semestre. Pero eso no significa que Apple se duerma en los laureles. En este primer semestre se han publicado dos grandes versiones de iOS 17: 17.4 y 17.5 con poco más de un mes de diferencia entre ellas. Vamos a ver que nos traen en el apartado de la seguridad.

Hay que comentar que en la versión 17.4 prepara al sistema operativo para la apertura a tiendas de terceros, promovida por la legislación europea (Ley de Mercados Digitales) que está ideada para promover la libre competencia. Esto constituye un punto de inflexión importante cuyos matices en el aspecto de la seguridad están aún por ver.

17.4 nos trae una mejora en la función de protección de dispositivo robado. En particular, cuando el iPhone entra en este modo someterá diversas acciones, como el acceso a contraseñas y datos, a la autenticación con biometría. Es decir, si alguien conoce nuestro código de acceso al iPhone, éste no será suficiente y solicitará una comprobación adicional de carácter biométrico para asegurar que es el legítimo dueño el que está accediendo al dispositivo.

Otra curiosidad es que si se intenta cambiar el AppleID del dispositivo, se tendrá que esperar hasta una hora. En ese momento, el sistema volverá a pedir la autenticación biométrica para asegurar que la operación es lícita. Dicha técnica se conoce como Security Delay. 17.5 nos trae una curiosa funcionalidad respecto a la privacidad. Si recordamos, los Apple Tags son dispositivos cuyo uso legítimo es bastante útil. Nos permiten encontrar fácilmente cosas como llaveros, carteras, mochilas, etc. Incluso dejarlos en un vehículo nos permite realizar un monitoreo de su posición en caso de robo. El problema con estos dispositivos es que no pueden discernir si el uso que les están dando es ético o se están empleando para realizar un seguimiento ilegal y cuestionable.

A partir de 17.5 el sistema nos avisará en caso de que estemos cerca de un Apple Tag que no sea conocido. La idea es que si pasamos un tiempo cerca de ese dispositivo (nos movemos con él) avise de la cercanía y de que está activo.

El próximo semestre se publicará, previsiblemente, iOS 18 cuyas versiones de desarrollo ya se están probado y veremos qué nuevas novedades nos trae.

Vulnerabilidades y versiones publicadas en el primer semestre de 2024

Repasamos las actualizaciones de seguridad del sistema operativo iOS que nos ha traído el primer semestre de 2024. Recordemos que dejamos el semestre anterior con las versiones iOS 17.2.1, 16.7.4 e 15.8.

La salida de nuevas versiones se alargó hasta el 22 de enero. El año se estrenó con 15.8.1, 16.7.5 y 17.3.

Respectivamente, dos, nueve y 20 parches, de los cuales nueve reparan vulnerabilidades que permitían la ejecución de código arbitrario. Hay que destacar que el componente estrella (más afectado) es WebKit (Safari).

El 8 de febrero nos encontramos con 17.3.1, pero no trae parches de seguridad. Se trata de un grupo de corrección de errores de programación y mejoras en la funcionalidad de los sistemas.

El 5 de marzo sale 15.8.2 sin correcciones de seguridad. Ese mismo día los usuarios de la versión 16 se despiertan con un grupo de parches de seguridad y no precisamente pequeño. Hasta 19 vulnerabilidades son corregidas en 16.7.6, aunque solo una de ellas reviste gravedad.

Pero el plato fuerte del día es el estreno de la esperada versión 17.4 con una lista bastante nutrida de parches de seguridad: hasta 39 correcciones. Cuatro de ellas solucionando ejecuciones de código arbitrario.

Marzo no se despide sin parches. El 21 de ese mes hacían su aparición 17.4.1 y 16.7.7 con idénticas correcciones y graves: parches para los componentes WebRTC y CoreMedia que permitían ejecución de código arbitrario.

Abril fue un mes tranquilo, pero el día 13 de mayo trajo una gran actualización, nada más y menos que iOS 17.5, con 42 parches, 13 de ellos asociados a ejecución de código arbitrario.

Paralelamente, se publica 16.7.8 con la mitad de los parches, 21, siendo siete de ellos de carácter grave.

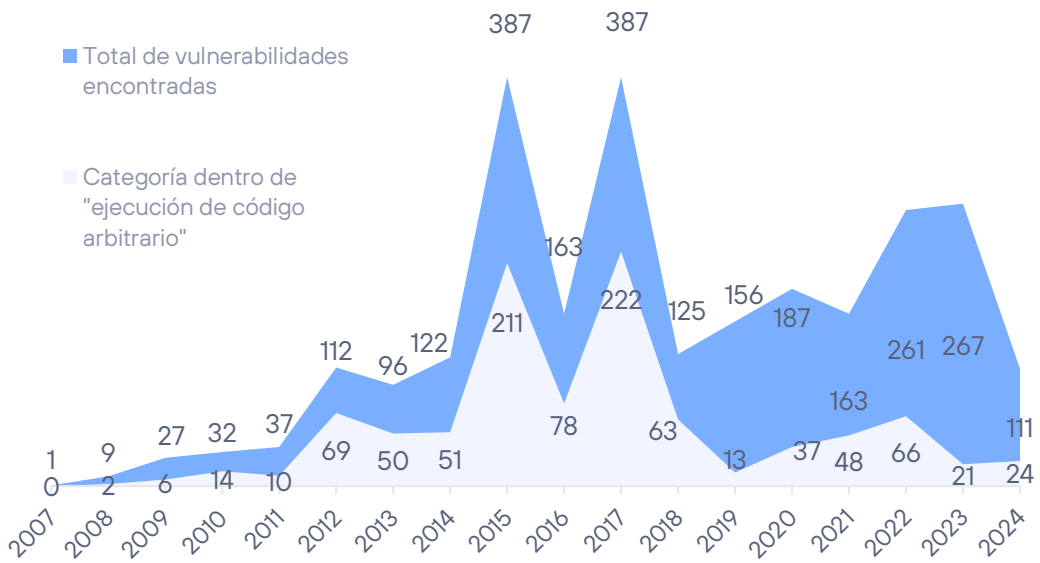
Cerramos el semestre con la aparición de 17.5.1 el 20 de mayo pero no trae ninguna actualización de seguridad.

Evolución de vulnerabilidades en iOS durante el primer semestre de 2024

El primer semestre de 2024 se ha cerrado con 111 vulnerabilidades únicas parcheadas, alrededor de dos docenas consideradas de alto riesgo, con posibilidad de ejecutar código arbitrario. Ya son más que todas las de alto riesgo encontradas en 2023.

VULNERABILIDADES EN IOS 2024-H1

Evolución de vulnerabilidades por año



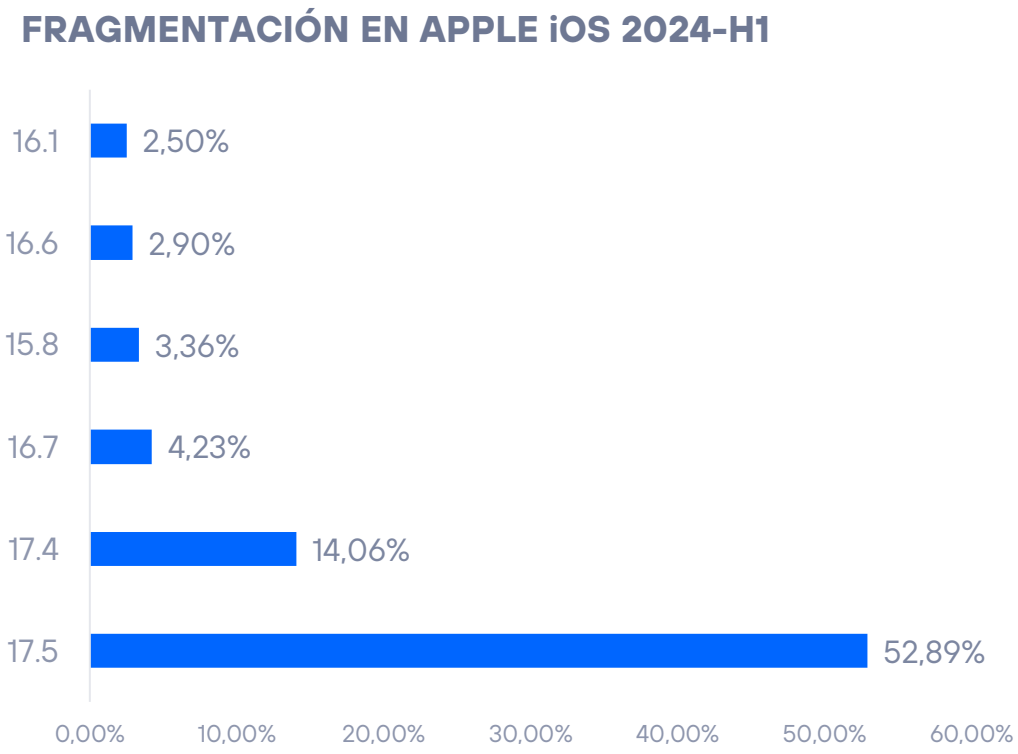
Fragmentación de versiones durante el primer semestre de 2024

Como es tradición, la fragmentación nunca ha sido un problema para los desarrolladores de iOS. La ventaja de contar con una plataforma homogénea es indiscutible 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.

Como es habitual en el ciclo de versiones de Apple, iOS 15 ha desaparecido prácticamente con solo una cota de poco más del 3%, siendo las versiones que priman la 17 y 16 que comienza a eclipsar, siendo la 17.5 y 17.4 el grueso del ecosistema iOS.

Tan solo las distintas subramas persisten, procedentes de terminales cuyos usuarios aún no han actualizado a versiones de ramas superiores.



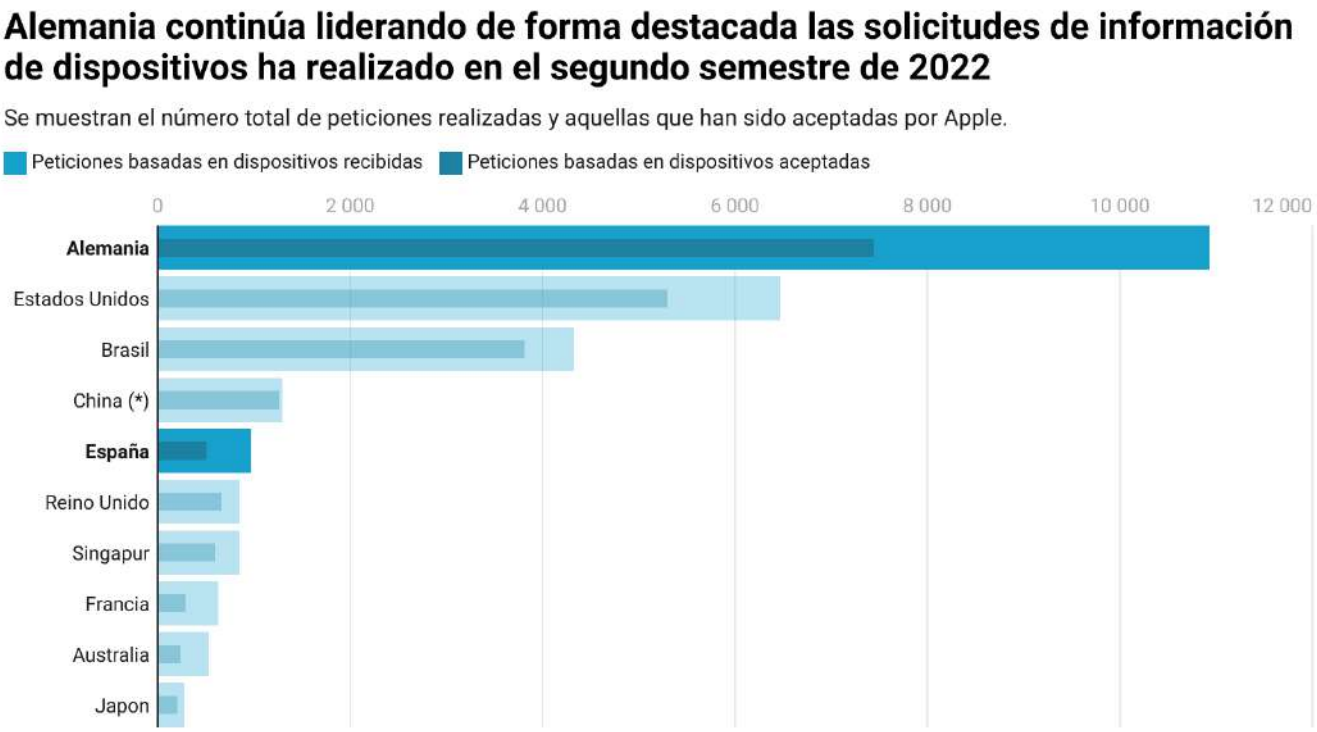
Informe de Transparencia de Apple

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 segundo semestre del año 2022 (el último publicado por Apple a fecha del primer semestre de 2024)** 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.

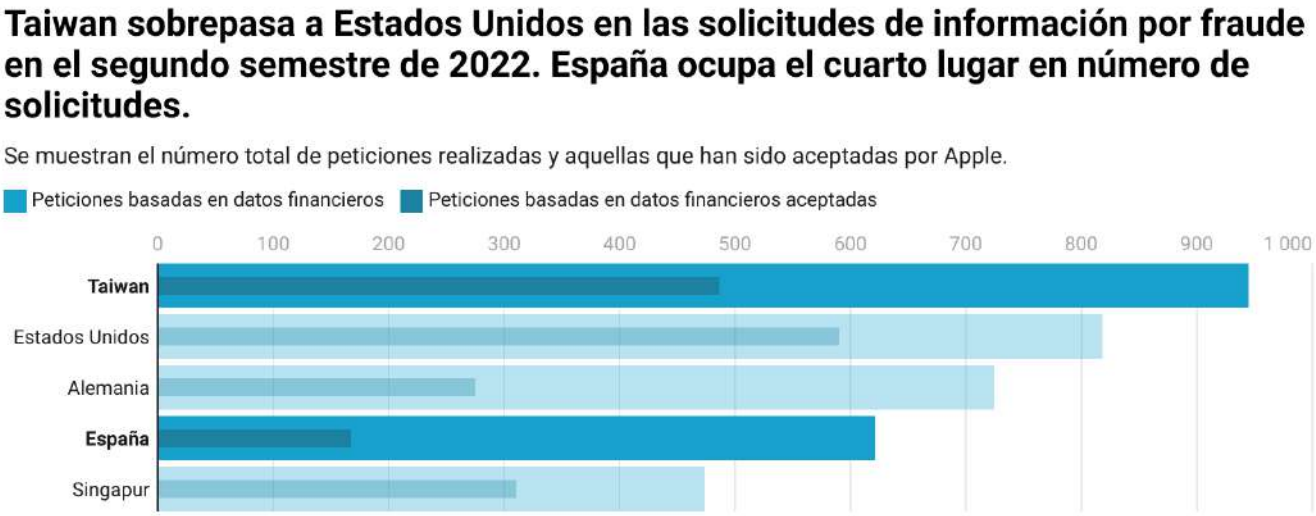


Dentro de este Top10 el grado de aceptación varía desde el 45% para las peticiones de Australia al 97% para las correspondientes a China. Este liderazgo de Alemania se traslada por primera vez también al número de dispositivos sobre los que solicita información con más de 100.000 dispositivos.

Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

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.

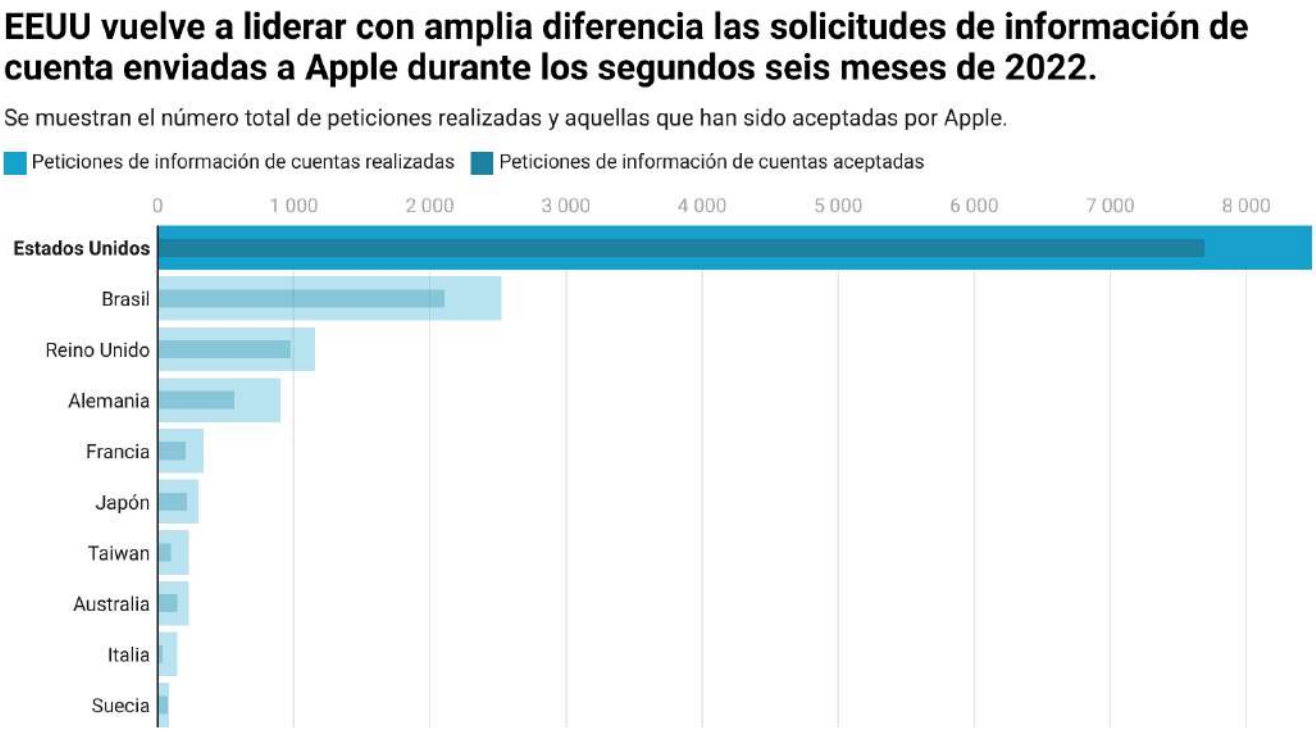


El grado de aceptación entre los 5 paises con mayor volúmen varía desde el 27% para las peticiones de España al 72% para las correspondientes a EEUU.

Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

Peticiones basadas en cuentas

Se realizan, desde los gobiernos, 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...).



De las 76 peticiones realizadas por España, el undécimo país con mayor número de solicitudes, solamente 33 fueron aceptadas (43%).

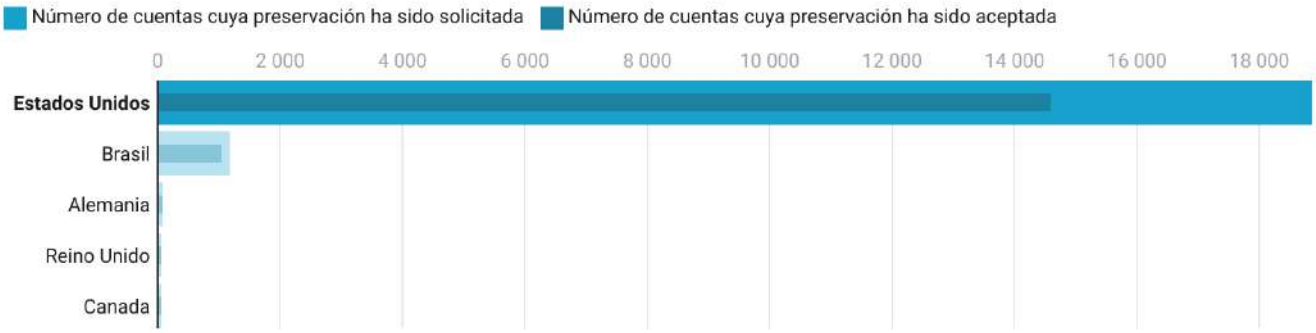
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

Peticiones relacionadas con la preservación de cuentas

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

EEUU multiplica por más de 20 a cualquier otro país, en las solicitudes de preservación de cuentas a Apple, durante los primeros segundos 6 meses de 2022.

Se muestran el número total de cuentas cuya preservación ha sido solicitada y aquellas cuya preservación ha sido efectivamente realizada por Apple.



España no emitió ninguna solicitud de preservación de cuenta durante todo el 2022. Solamente EE.UU. parece usar esta capacidad de forma efectiva.

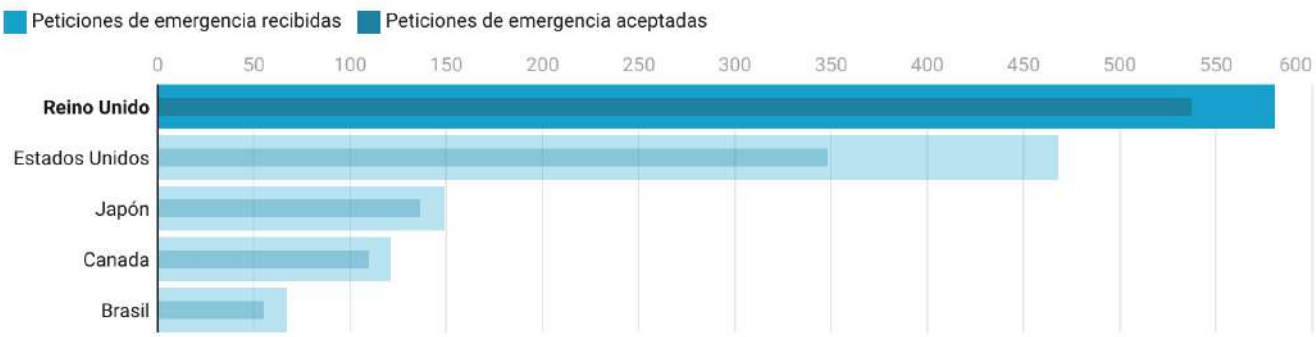
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

Peticiones por emergencias

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

UK vuelve a ser el país que más peticiones de acceso a cuentas por emergencia solicita en el segundo semestre de 2022, seguido de cerca por USA.

Se muestran las peticiones de acceso a cuenta por emergencia realizadas y aquellas aceptadas por Apple.



España, que ocupa el puesto 25 en el ranking, emitió 2 solicitudes de acceso a cuenta por emergencias y todas fueron aceptadas (100%).

Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

Peticiones relacionadas con la retirada de apps del market

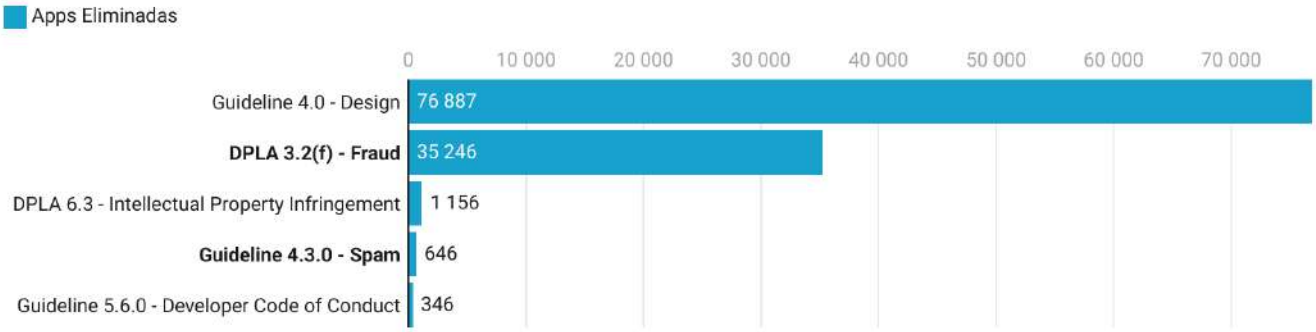
A mediados de 2024 Apple ha publicado su compromiso con la generación de un informe de transparencia específico para su App Store en el que ha ampliado la información relativa a la retirada de apps del market poniendo a disposición del público una información interesante en este caso anual (2023) que analizaremos a continuación.

Dando continuidad a lo analizado en otros informes semestrales, comenzamos por explorar las retiradas de aplicaciones que violan la ley soberana del país/región solicitante.

A continuación, veremos un interesante desglose de las retiradas de aplicaciones tanto por incumplimiento de normativa interna de Apple dentro del proceso de revisión para llegar al *market* como por incumplimiento del acuerdo de desarrollador de aplicaciones de Apple.

Fraude y Spam continúan entre las 5 causas principales de eliminación de apps del market de 2023 por incumplimiento de normativa o políticas de desarrollo de Apple.

Se muestran las Apps eliminadas y la normativa específica que se ha incumplido



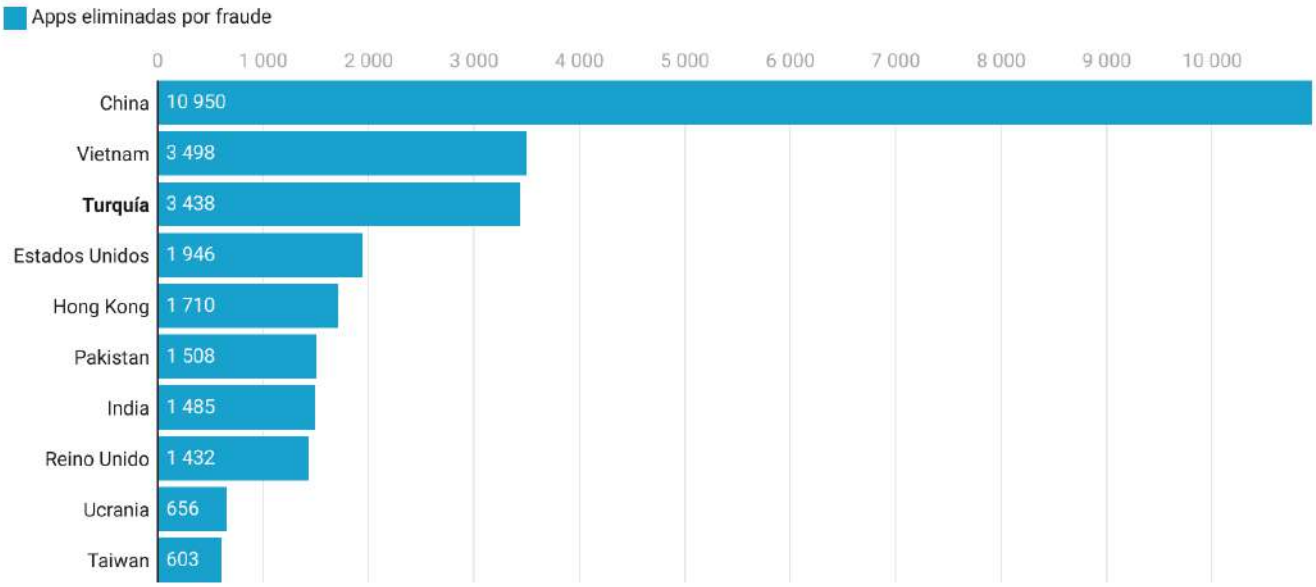
Llama la atención la reducción de casi el 50% de eliminación por problemas de diseño respecto a 2022. Más info en: https://developer.apple.com/support/terms/apple-developer-program-license-agreement/ y https://developer.apple.com/app-store/review/guidelines/

Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

Centrándonos en las categorías más relacionadas con la ciberseguridad, podemos ver un desglose de los 10 países con desarrollos con más infracciones por spam y fraude.

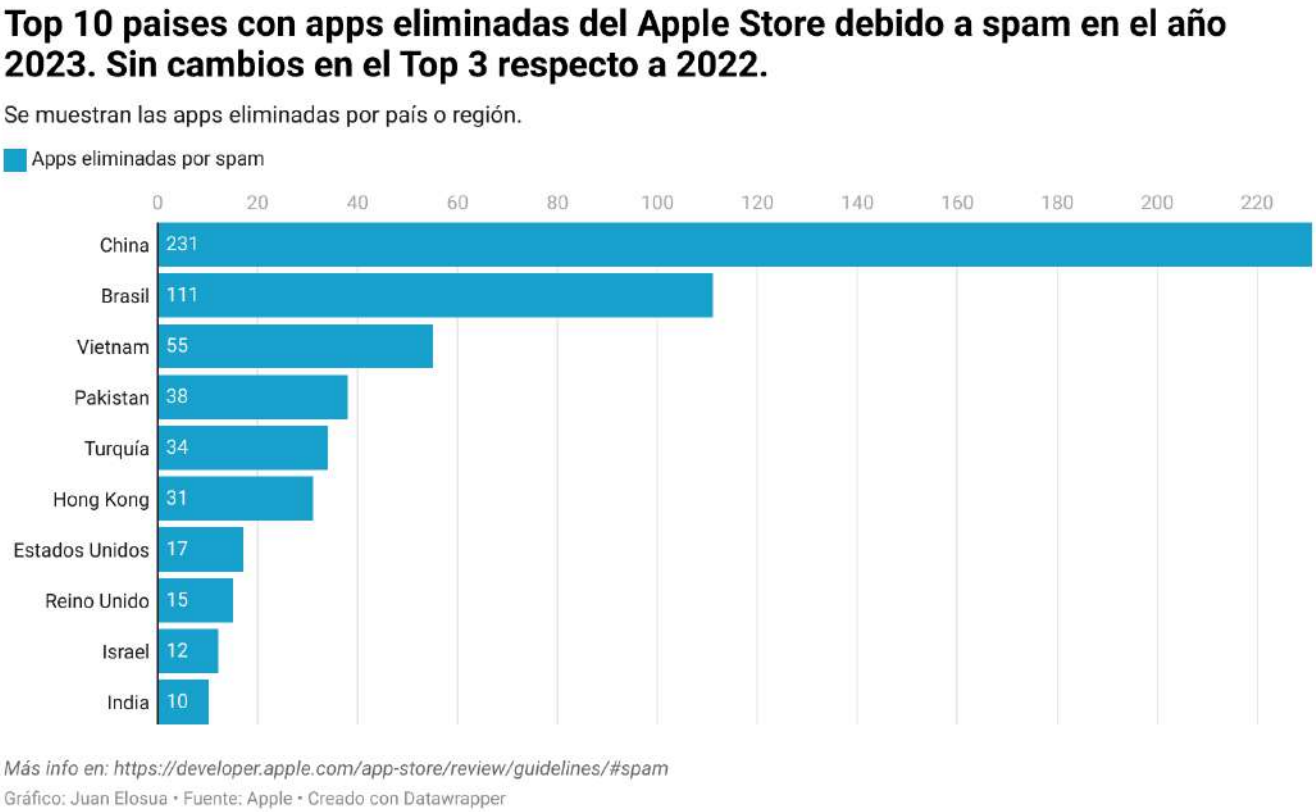
Top 10 paises con apps eliminadas del Apple Store debido a fraude en el año 2023. Turquía multiplica por 2 sus números respecto a 2022.

Se muestran las apps eliminadas por país o región.



Más info en: https://developer.apple.com/support/terms/apple-developer-program-license-agreement/#ADPLA3.2

Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper



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 allí, o que haya más fraude más en estas localizaciones, la interpretación es libre. A continuación, algunas conclusiones basadas en nuestro análisis:

- El gobierno alemán es el que más solicitudes ha generado para obtener información sobre dispositivos desde que hacemos este seguimiento. **Este liderazgo se extiende por primera vez, en el segundo semestre de 2022, al número concreto de dispositivos incluidos en las solicitudes**.
- **Taiwán rebasa por primera vez a Estados Unidos en las solicitudes de información de cuentas por fraude** en el segundo semestre de 2022, **España ocupa el cuarto lugar, aunque con un grado de aceptación por parte de Apple muy bajo (27%)**.
- Estados Unidos solicita con diferencia más que cualquier otro país la preservación de cuentas y el acceso a los datos alojados en ella. Lo que continúa destacando de nuestro análisis es que **Brasil sigue en un sólido segundo lugar de una forma destacada duplicando las solicitudes respecto al tercero**.
- **Reino Unido continúa liderando las solicitudes de acceso a información de cuentas por situaciones de emergencia**, aquellas donde se puede evitar un peligro de muerte o daño serio a individuos. Resulta sorprendente a raíz de los volúmenes de acceso a cuentas de EE.UU. Esto refuerza la teoría de que exista un procedimiento de lanzamiento de este tipo de solicitudes por parte de su departamento de exteriores.
- China continúa siendo el país que más retirada de *apps* solicita en el App Store. La diferencia es enorme con el resto del mundo. En este año gracias al nuevo informe de transparencia del App Store

sabemos que 1.067 del total de 1.285 aplicaciones retiradas, se deben a juegos que no disponen de la aprobación del organismo regulatorio chino. **Corea del sur pasa a ocupar una destacada segunda posición**, veremos si es una tendencia o algo anecdótico con los próximos datos de Apple.

- Vemos que, dentro de las aplicaciones retiradas del Apple App Store, el **fraude y el spam continúan formando parte del "Top 5" de categorías de infracciones cometidas por desarrolladores en 2023 siguiendo la línea de lo visto en 2022**. Llama la atención el descenso de infracciones relacionadas con problemas de diseño reduciéndose en casi la mitad respecto a 2022.
- Por último, señalar que **Turquía ha visto multiplicado por 2 las apps eliminadas por fraude por parte de Apple**, como en el caso de Corea del Sur habrá que esperar a los datos de 2024 para revisar su relevancia.

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

Nuevas características de seguridad

Aún continuamos con Android 14, que a fecha de elaboración de este informe lleva 54 revisiones en total desde su salida el 4 de octubre de 2023. Android 15 solo existe en su forma de beta para desarrollo y no se espera su liberación hasta después del verano, como viene siendo habitual.

No tenemos muchas novedades en el apartado de seguridad más allá de los parches publicados, pero podemos asomarnos a la ventana de características nuevas que traerá Android 15 próximamente en avanzada.

La característica estrella es la nueva **sandbox de privacidad**. La apuesta de Google para salvaguardar la privacidad del usuario con un rastreo con restricciones en las cookies de terceros, etc., que también está pensada para el navegador web.

Tal y como reza en el sitio web de Google dedicado a esta tecnología: "Nuestra propuesta es llevar Privacy Sandbox a Android y proporcionar una ruta clara para mejorar la privacidad del usuario sin poner en riesgo el acceso al contenido y los servicios sin cargo".

En el apartado de desarrollo, se pone a disposición de los desarrolladores la API de integridad de archivos (FileIntegrityManager) que permitirá proteger vía firma criptográfica la integridad de los archivos que elijamos.

En el próximo informe desgranaremos estas nuevas mejoras y las que vengan con la salida previsible de Android 15.

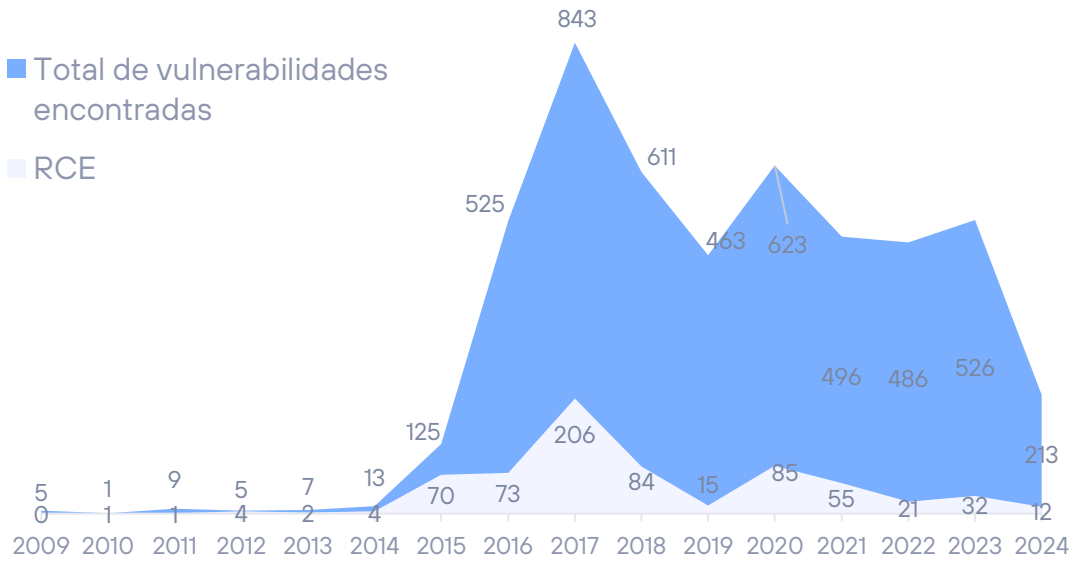
Vulnerabilidades

Android publica un conjunto de parches cada mes, generalmente durante la primera semana. En este primer semestre de 2024 se han publicado seis boletines con una distribución de 59, 46, 38, 28, 29 y 13 parches o CVE únicos corregidos por mes.

En total, 213 parches (el semestre anterior fue de 297); 12 de ellos considerados críticos (32 en todo el año anterior).

Hay que hacer notar, que 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 EN ANDROID 2024-H1
Evolución de vulnerabilidades por año



Fragmentación en sistemas Android

La última publicación de *Statcounter* a fecha de edición de este informe nos indican que la versión más implantada de Android es la 14, con un share del 25.64%, seguida por la 13 con un share de 22.29%.

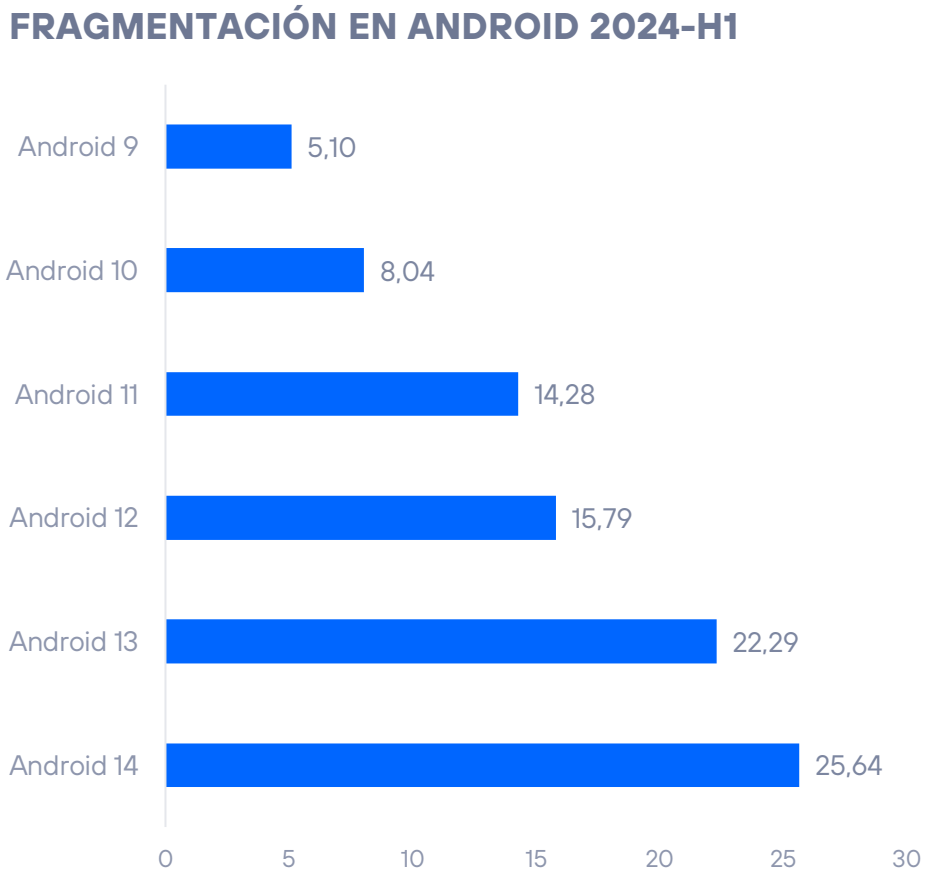
Es típico el momento de mayor pico en la versión actual, la 14, estrenada en octubre, que comenzará a declinar en cuanto se libere 15, algo que le está ocurriendo a Android 13 cuyo share ha bajado en algo menos de 14 puntos de cuota de mercado.

Las versiones de Android anteriores a la versión 12 (incluida, sistema que apareció en septiembre de 2020) ya no tienen soporte de actualizaciones.

Esto es un aspecto notablemente negativo: la existencia de sistemas sin soporte alguno pero que continúan en funcionamiento activo sin recibir actualizaciones de seguridad.

Por ejemplo, Android 12 todavía cuenta con un 15.79% de la tarta (un buen pedazo) al igual que Android 11 con un 14.28%. Entre estos dos sistemas, repetimos: sin soporte, representan un 30% de la población con teléfonos Android.

Es más, todavía aparecen la versión 10 y 9 con un 8.04% y 5.1% respectivamente. El resto de cuota no representada (algo menos de un nada desdeñable 10%) lo ostentan versiones incluso más antiguas, como 8.0 y 8.1 Oreo e incluso 7.0 Nougat.



VULNERABILIDADES DESTACABLES

Comentamos en esta sección algunas de las vulnerabilidades notables a nuestro juicio, de este primer semestre de 2024.

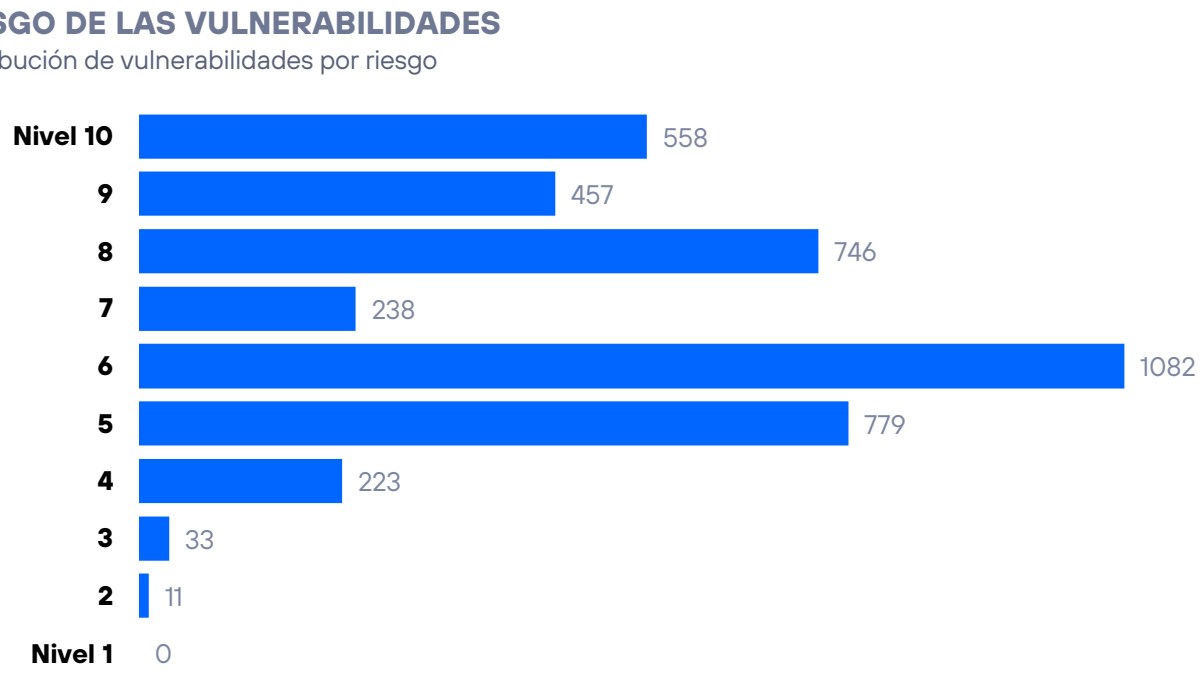
CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2024-4577	PHP en Windows	La funcionalidad 'Best-Fit' en Windows cuando se usa PHP en modo CGI permite ejecución de código.	9.8
CVE-2024-21764	Rapid Scada	Un atacante podría leer archivos confidenciales del servidor, escribir archivos en el directorio Rapid Scada (logrando así la	9.8

		ejecución del código), obtener acceso a sistemas y datos confidenciales, etc.	
CVE-2024-21767	Sistema de control de acceso WS203VICM	La vulnerabilidad crítica podría permitir a un atacante remoto eludir el control de acceso de Commend WS203VICM mediante la creación de una solicitud maliciosa.	9.4
CVE-2024-21899	QNAP OS	La explotación de la vulnerabilidad permite a un atacante sin autenticar acceder a un dispositivo NAS de manera remota	9.8
CVE-2024-22252 y CVE-2024-22253	VMware Workstation/Fusion y ESXi	La explotación requiere privilegios administrativos locales en una máquina virtual, pero podría permitir que un atacante ejecute código como el proceso VMX de la máquina virtual en el host. En Workstation y Fusion, esto podría provocar la ejecución de código en la máquina host.	9.3
CVE-2024-23897	Jenkins	Un fallo en args4j permite leer ficheros de forma arbitraria y por tanto, ejecutar código. Se publicó prueba de concepto.	9.8
CVE-2024-24691	Zoom - Windows	Un fallo en la validación de parámetros de entrada en la aplicación de Zoom para Windows permite que un usuario remoto sin autenticar pueda conseguir escalar privilegios en el sistema anfitrión.	9.6
CVE-2024-26305	ArubaOS	Vulnerabilidad de tipo Buffer Overflow sobre el demonio "Utility" que permite a un atacante sin autenticar ejecutar código arbitrario remotamente sobre el protocolo usado por Aruba para administrar puntos de acceso y sistemas de monitorización de redes inalámbricas.	9.8
CVE-2024-27322	Lenguaje de programación R	Permite la ejecución de código arbitrario a través de archivos RDS y RDX especialmente diseñados. R es un lenguaje ampliamente utilizado en sectores críticos por su facilidad de uso para el análisis estadístico y la minería de datos.	8.8
CVE-2024-27956	Wordpress Valvepress	En versiones anteriores a la 3.9.2.0 se puede eludir el mecanismo de autenticación de este plugin para realizar ataques de SQLi que podrían derivar en la creación de cuentas de administrador en el sitio web.	9.9
CVE-2024-3094	Xz Utils	Las versiones 5.6.0 y 5.6.1 de esta librería de compresión de datos contienen código malicioso que puede autorizar el acceso remoto no autorizado a través de SSH utilizando un payload que modificaba las rutinas de descifrado del servidor OpenSSH para permitir que un atacante remoto pudiera autenticarse	10.0
CVE-2024-36266	PowerSys, controlador de sistemas de teleprotección para	La aplicación afectada no protege suficientemente las respuestas a las solicitudes de autenticación. Esto podría permitir que un	9.3

	líneas de alta tensión SWT 3000 de Siemens	atacante local eluda la autenticación y obtenga así privilegios administrativos para los dispositivos remotos administrados.	
CVE-2024-37036	RTU Schneider Electric	Existe una vulnerabilidad de escritura fuera de los límites que podría provocar una omisión de autenticación al enviar una solicitud POST con formato incorrecto y se establecen parámetros de configuración particulares.	9.8

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.

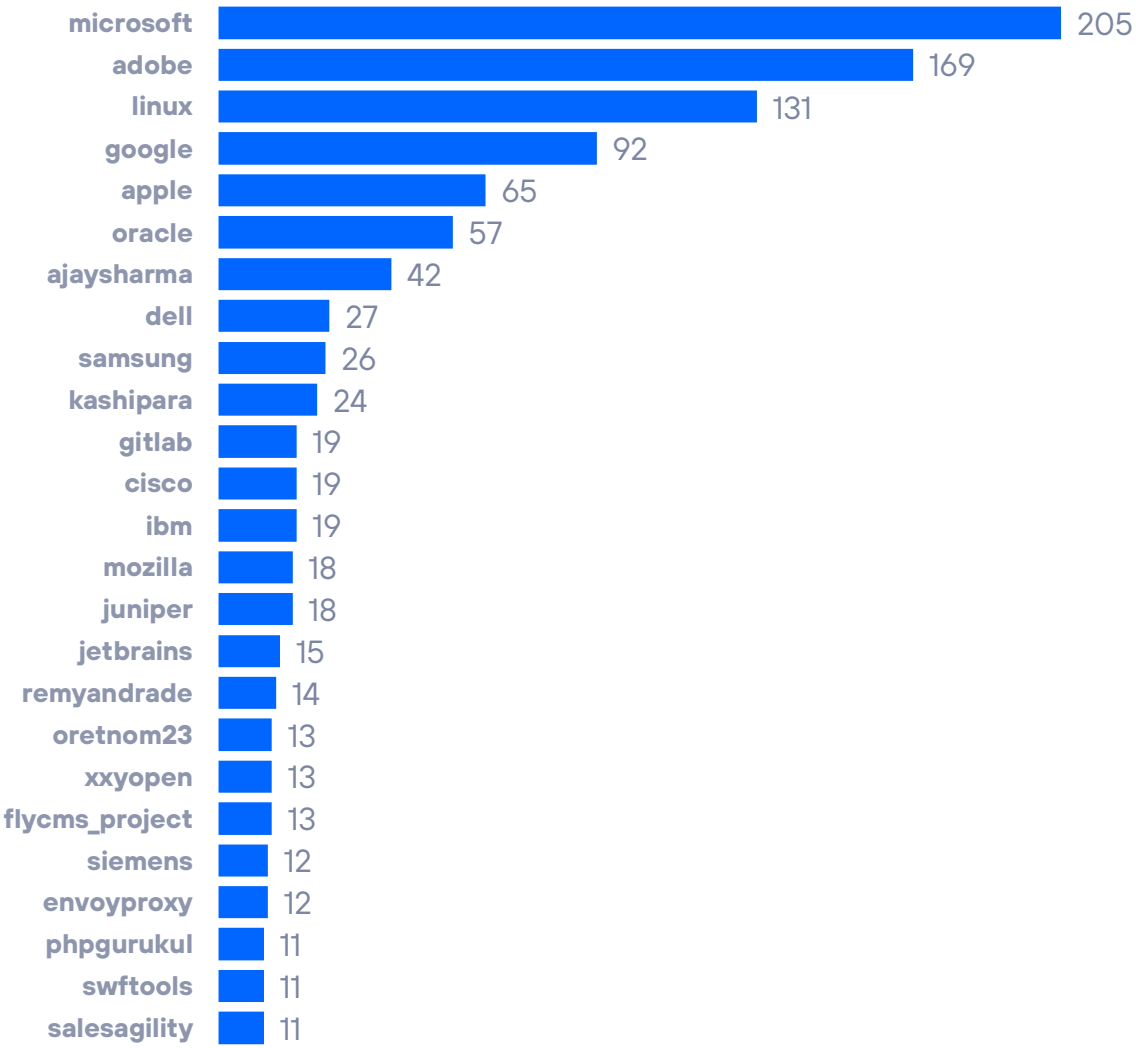


Top 25 compañías con más CVE acumulados

Durante el primer semestre de 2024, Microsoft ha liderado con diferencia por número de vulnerabilidades conocidas, seguido de Adobe y Linux (de forma genérica). En general, es habitual que Microsoft, Google y Oracle estén siempre entre los primeros en número de vulnerabilidades pero este semestre nos encontramos con Adobe con un gran número de fallos.

VULNERABILIDADES POR FABRICANTE

Top 25 fabricantes por CVE acumulados



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 2024

Sea Turtle - se dedica a morder cables de internet

Este grupo, también conocido como “Teal Kurma” y “Cosmic Wolf”) respaldado por el gobierno turco, ha sido detectado llevando a cabo múltiples campañas de espionaje en los Países Bajos, centrándose en las empresas de telecomunicaciones, los medios de comunicación, los proveedores de servicios de Internet (ISP) y los sitios web kurdos.

Antes de este cambio de objetivo, el grupo se centraba en Oriente medio, Suecia y Estados Unidos, utilizando TTP relacionadas con el secuestro de DNS y redirecciones de tráfico para hacer ataques MiM.

En su viaje por costas neerlandesas, la tortuga ha mostrado especial interés por datos de inteligencia económica y política y, específicamente, por intereses e información kurda.

Sus TTP no son especialmente complejas o novedosas. El acceso inicial en los ataques observados se logra mediante el uso de cuentas de cPanel comprometidas para establecer un tunel SSH en la infraestructura de destino. Después utilizan una Shell de código abierto para una conexión TCP inversa para conseguir capacidades de Command & Control.

Más información en https://www.huntandhackett.com/blog/turkish-espionage-campaigns

Cozy bear – Políticamente incorrectos

Conocidos también como "APT29", este grupo ha sido observado por investigadores de Mandiant empleando una nueva backdoor denominada "Wineloader". Dicha backdoor fue detectada a finales de enero de 2024, pero no se consiguió asociar su uso a ningún grupo APT conocido. Sin embargo, el objetivo de la campaña en el que se utilizó hacía pensar que podría ser APT29, especializado en objetivos diplomáticos y embajadas.

Un mes más tarde, se volvió a detectar esta puerta trasera (una nueva versión) en una campaña de phishing contra objetivos políticos. Concretamente, mensajes que se hacían pasar por una invitación del partido CDU alemán a una cena. La puerta trasera tiene características y funciones de uso común en otras herramientas de APT29, lo que terminó por asociar la campaña y la backdoor a este grupo.

Por cierto, Cozy Bear fue el grupo autor del ataque a Solarwinds

Más información en: https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties

Sandworm – Bajo la arena

El gusano ha vuelto. Los creadores de Black Energy han sido descubiertos haciendo el mal bajo la máscara del hacktivismo. En este caso, el grupo ha sido detectado empleando varios canales de Telegram para amplificar la comunicación de sus acciones a través de narrativas próximas a la propaganda estatal. Sin embargo, todos cometemos errores. Los canales de Telegram compartían acciones del grupo ya realizadas... hasta que, en un momento dado, uno de los canales de Telegram comunicó una acción que aún no se había llevado a cabo. En ese momento quedó claro que los canales de Telegram y el APT44 eran lo mismo (o muy parecido).

Pero ¿por qué hacerlo así y no anunciarlo directamente? Los investigadores de Mandiant explican que parece un ensayo de transmisión de la información para fingir un apoyo popular a este tipo de acciones de grupos APT esponsorizados por los estados y

sus servicios de inteligencia. Somos animales sociales. Algo contrario a nuestra forma de pensar, pero apoyado por una parte importante de la sociedad genera menos rechazo o más dudas que ese mismo "algo" apoyado por nadie o casi nadie.

Bienvenidos a las estrategias híbridas de control de las narrativas.

Más información en: https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-pose-as-hacktivists-in-water-utility-breaches/

Unfading Sea Haze - Terror en la niebla

Seis años, seis, ha tardado el ecosistema de ciberseguridad en detectar a este grupo. Desde 2018 se ha encargado de "visitar" a entidades militares y gubernamentales en la zona del Mar de China Meridional.

Y cómo han conseguido estar ocultos durante tanto tiempo, dos conceptos:

Por un lado, este grupo comparte características con APT41, pero tiene diferencias que lo distinguen claramente de nuestros ya conocidos "Double Dragon". Esta compartición es, por otro lado, algo común en los grupos esponsorizados por los estados.

Por otro lado, trabajan fino. Empiezan con campañas de spear-phishing bien preparadas, abusan de servicios legítimos (instalando malware sin necesidad de tener un fichero descargado, compilando desde memoria con MSBuild) y emplean herramientas propias. Si a eso le unimos paciencia y capacidad para mejorar lo que ya funciona, tenemos un grupo que lleva evadiendo controles desde hace mucho tiempo.

Más información en: https://www.bleepingcomputer.com/news/security/unfading-sea-haze-hackers-hide-on-military-and-govt-networks-for-6-years/

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.

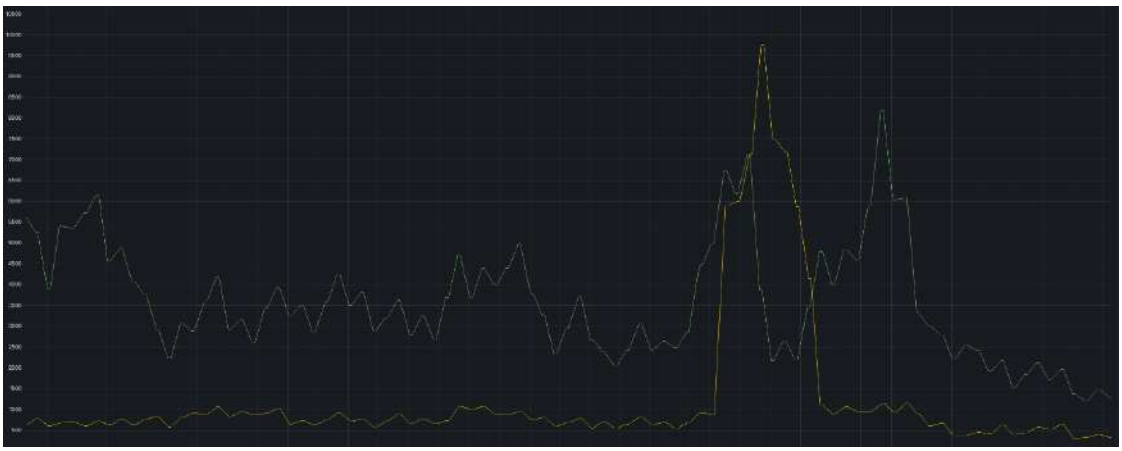
Esta variabilidad puede generar ligeras discrepancias en los datos mostrados en este apartado si se comparan entre semestres.

Análisis de la información

A continuación, vamos a comentar una campaña que nos ha parecido especialmente interesante, centrando este breve análisis en el país que ha protagonizado el mayor número de acciones registradas: Bulgaria.

Campaña de descubrimiento

El día 22 de mayo, Aristeo detectó un comportamiento inusual dentro de su red de señuelos:



La actividad que se observa en la gráfica es una ampliación de Aristeo sobre los dos primeros señuelos en los que se detectó la anomalía en la actividad. No daremos más datos de ambos señuelos, pero digamos que cada uno estaba recibiendo interacciones como se podría esperar. Aumentos, descensos... todo dentro de lo "normal" que puede ser el panorama de los ciberataques a nivel global. Sin embargo, a partir del día 22 de mayo aumentó la actividad de manera anómala. En uno de ellos se observa como la campaña tiene dos picos

bien diferenciados, mientras que, en el otro, con mucha menos actividad, el aumento es más que apreciable. La campaña finalizó el 3 de julio.

¿El origen de la campaña? El epicentro se detectó en Bulgaria, pero países más al Este aumentaron también su actividad.

Posición	Previo		Campaña		Posterior	
#	País	%	País	%	País	%
1	Países Bajos	36.58	Bulgaria	30.28	USA	39.16
2	USA	27.55	USA	19.91	China	9.90
3	Bulgaria	8.57	Rusia	14.27	Países Bajos	8.92
4	India	5.70	Países Bajos	11.31	Rusia	8.27
5	China	5.69	Brasil	6.65	UK	6.50
6	UK	4.59	India	3.94	India	6.45
7	Rusia	3.69	China	3.87	Bulgaria	6.22
8	Irlanda	2.80	Hong Kong	3.65	Irlanda	5.03
9	Alemania	2.40	UK	3.56	Singapur	5.00
10	Vietnam	2.30	Irlanda	2.57	Baréin	4.54
MEDIA	186.376,50		294.319,38		172.225,44	

Se puede observar que la media de eventos del antes y el después el similar, pero durante la campaña ascendió un 58%. Si nos fijamos en los países que más aumentan su representatividad en el Top-10 de países con más eventos, observamos que Bulgaria supera con mucho los límites de lo esperado. Que la media de eventos aumente un 58% y su representatividad aumente desde el 8.57% al 30.28% indica la magnitud de la campaña. Otro país que aumenta sensiblemente su representatividad es Rusia, aunque no de la manera en que lo ha hecho Bulgaria.

¿Objetivos y tipo de actividad? De todo. Aunque el patrón de detección en ambos señuelos es distinto, no hay una razón aparente para que esto haya ocurrido, más allá de que el tipo de exposición de cada señuelo (porque no se parecen demasiado) haya determinado la manera de llegar de los orígenes registrados.

Puerto destino	Conteo	Servicio-Exploit
8728	4.485	MikroTik Router - CVE-2023-30799
445	3.169	Samba
1900	1.284	SSDP
27017	1.049	MongoDB
23	658	Telnet
3306	501	MySQL
8443	448	Apache Tomcat
80	376	Http
22	345	SSH
3389	318	RDP
53	262	DNS
5432	239	PostgreSQL
443	220	TLS
2222	214	Cognex In-Signt
222	202	Varios
22222	195	Varios
8080	181	Web proxy server
3128	173	Web proxy server
8888	171	Varios
8088	165	Varios

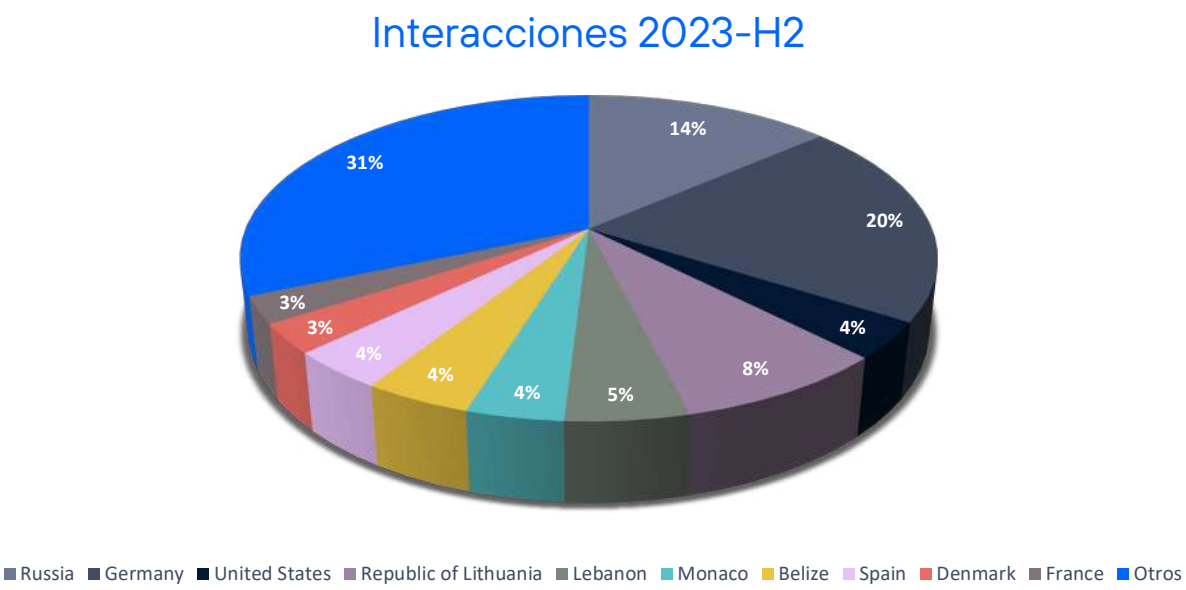
Estos son los puertos y servicios que más interés despertaron, pero no los únicos. Buscaron de todo en todos los señuelos de Aristeo que estaban activos. Por cierto, cuando decimos "de todo" es porque no hicieron un análisis inteligente previo de los objetivos. Algunos de los servicios y/o vulnerabilidades que intentaron explotar no tenían sentido por la sencilla razón de que **esa tecnología NO estaba presente en los señuelos**.

Aunque no podemos saber fehacientemente qué intenciones tenían los organizadores de la campaña, interacciones relativamente cortas y buscando cualquier servicio que pueda ser de interés, sin haber hecho antes una labor de footprinting o fingerprinting, podrían indicar una campaña para hacer un levantamiento de oportunidades que puedan ser aprovechadas más adelante.

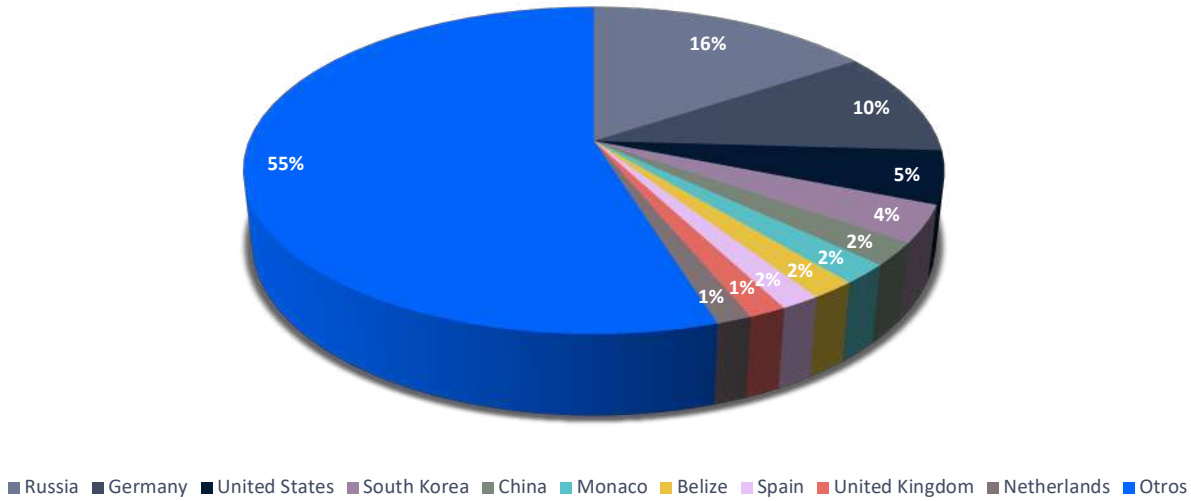
Veremos.

Y ahora, pasamos a la estadística general de la información registrada. En el primer semestre de 2024 se detectaron **más de 313 millones de eventos de ciberseguridad**. Esto supone un pequeño descenso respecto a los datos registrados en el segundo semestre de 2023, 322 millones, y un ascenso respecto al segundo trimestre de 2023, cuando se registraron poco más de 300 millones de eventos. No obstante, las cifras se mantienen en rangos muy similares.

La distribución por países sería la siguiente:



Interacciones 2024-H1



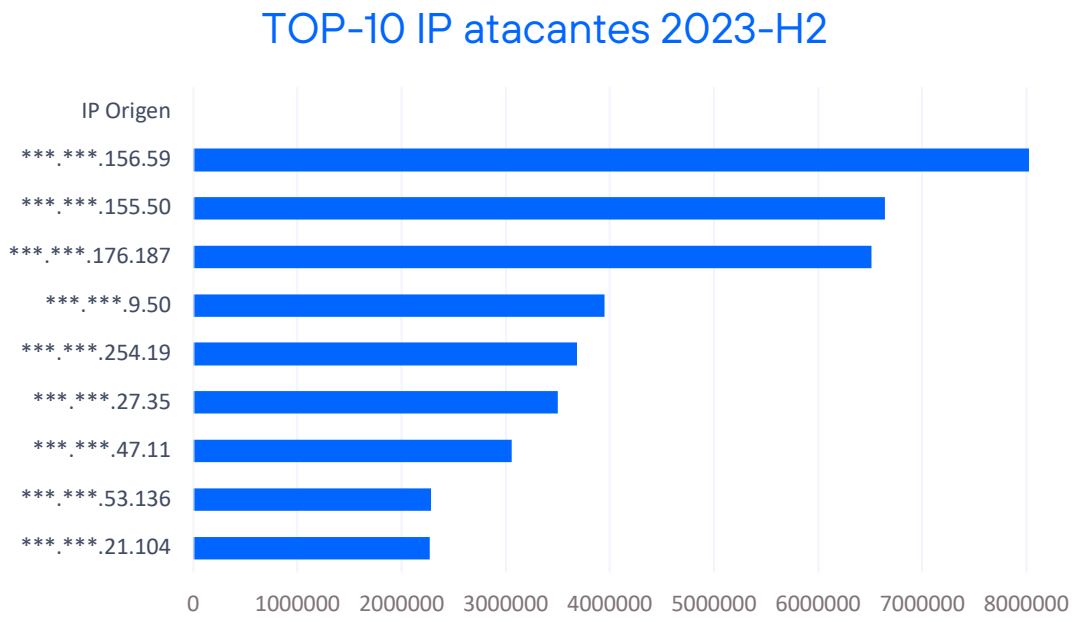
Pese a que se mantiene de manera general la dispersión de años anteriores, sucede algo curioso: ha habido una pérdida clara de representatividad del Top-10 en el total de eventos registrados. Mientras en el semestre pasado aglutinaban 183 millones de eventos, en este semestre el Top-10 ha registrado 141 millones de eventos. Este descenso, un 23% menos teniendo en cuenta el número de eventos totales de cada semestre, es bastante significativo. El Top-10 suele ser un baremo bastante representativo del total de los eventos (por eso lo seleccionamos y lo mostramos en los informes semestrales). Que el Top-10 haya perdido un 23% de representatividad de un semestre a otro supone un cambio significativo que debe ser interpretado correctamente.

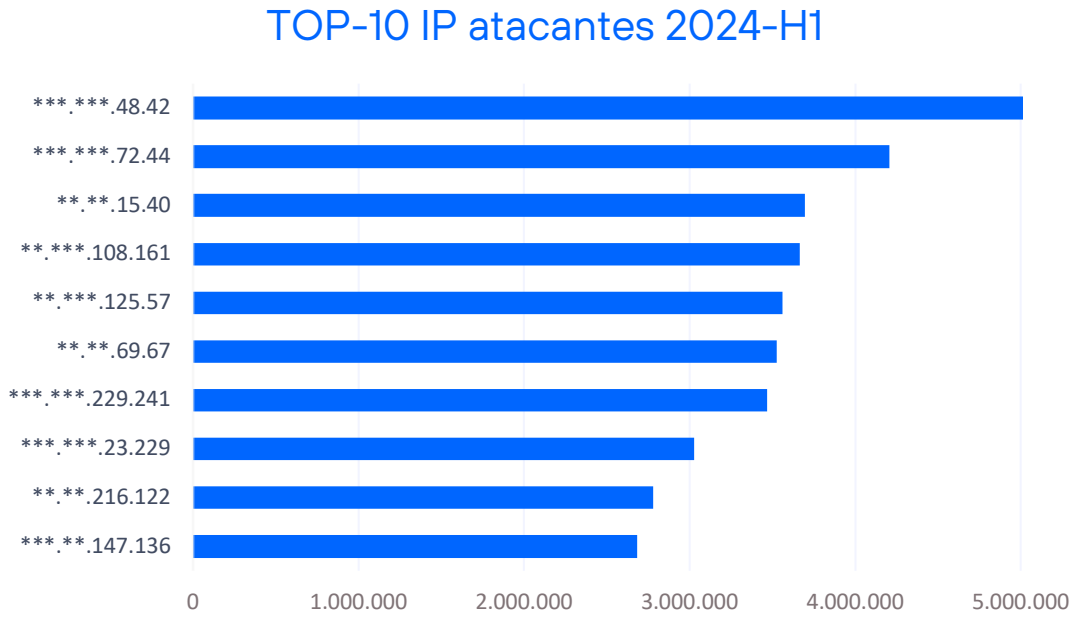
¿Dónde han ido los, aproximadamente, 36 millones de eventos que faltan? (los veremos en el último gráfico). Obviamente, distribuidos entre el resto de países, 88 este semestre, fuera del Top-10. Además, no hay un país o grupo pequeño de países que recojan esos eventos, lo que indica que no se trata de una campaña concreta, sino de un claro **aumento de la actividad a nivel general en todo el mundo**.

Aunque hemos afirmado que se registraron 9 millones de eventos menos este semestre, eso supone un descenso cercano al 3% entre todos los países registrados (98 países este semestre), lo que es una cifra muy baja y casi no-representativa del registro de eventos en medio año. Puede atribuirse a muchas las razones que justifiquen esa pequeña variación. Sin embargom, que el Top-10 de países con más eventos pierda la friolera de un 23% de representación de un semestre a otro y que, además, la actividad general no haya descendido de manera significativa, tiene seguramente mucho que ver con actividad más o menos notoria como la campaña de descubrimiento que hemos comentado antes en el documento.

Ahora vamos a ver las diez direcciones IP con más interacción con el sistema de Aristeo. En este semestre, el 85% de las 10 IP más registradas en nuestro sistema proviene del centro-norte-este de Europa. El lector atento habrá hecho el cálculo rápido: el 85% de 10 es 8.5, y quien haya leído el informe anterior ya sabrá por qué, pero vamos a explicarlo ¿Cómo se explica que media IP sea europea y la otra media no? Porque a veces hay direcciones IP geolocalizadas en un punto físico, pero que están delegadas o gestionadas desde otros sitios por interés de su propietario. Este caso se ha dado en el 70% del Top-10 de este semestre, con varios proveedores europeos de servicios gestionando IP localizadas en otros países de Europa que no son

el del proveedor. Sin embargo, una de estas direcciones IP del Top-10 está localizada en un país europeo, pero gestionada desde un país caribeño.



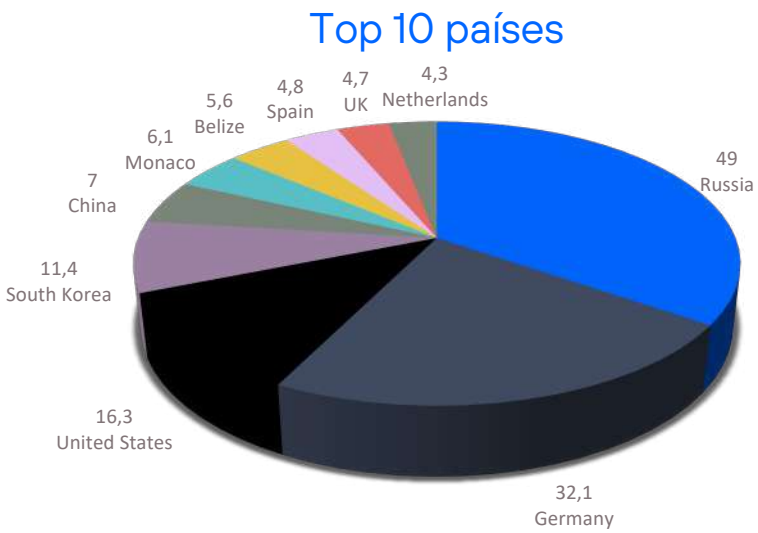


Si nos fijamos en los datos, de la misma forma que en el análisis en el Top-10 de países, el Top-10 de direcciones IP con más actividad pierde representatividad respecto al semestre anterior. Hablamos de un

porcentaje menos significativo a priori que en el caso del análisis por países, pero debemos tener en mente que los resultados analizados por países se distribuyen normalmente entre 100 países aproximadamente (98 este semestre) y si los analizamos por IP atacante, estamos hablando del orden de miles (y miles, y miles...).

En el análisis de IP hemos observado estos movimientos anteriormente, pero, unido a lo ya visto, el dato refuerza el análisis del que hablamos. El reparto más "equitativo" de impactos en la red de Aristeo junto con un descenso poco significativo del total de eventos indica un aumento global del interés.

A continuación, vemos cómo se reparten el *top 10* de los países registrados. Este semestre aumenta la influencia asiática, con Corea del sur y China (que salió del Top-10 el semestre pasado) como máximos representantes.



Vamos a aproximarnos de distinta forma a la representatividad del Top-10 de países. En este caso se puede observar que el descenso total de eventos de un semestre para otro ha sido de 47.7 millones de eventos. Si tenemos en cuenta que el descenso del global ha sido sólo de 9 millones, como indicábamos anteriormente, los otros 36 millones perdidos tienen que haber ido a algún sitio ¿A dónde?

Respuesta: al resto de países fuera del Top-10.

#	2023H2	2024H1	Diferencia
1	56,3M	49 M	-7,3 M
2	37,5 M	32,1 M	-5,4 M
3	23,3 M	16,3 M	-7 M
4	13,4 M	11,4 M	-2 M
5	11,7 M	7 M	-4,7 M

6	10,7 M	6,1 M	-4,6 M
7	10,6 M	5,6 M	-5 M
8	10 M	4,8 M	-5,2 M
9	8,1 M	4,7 M	-3,4 M
10	7,4 M	4,3 M	-3,1 M
Descenso total			47,7 M

El descenso refuerza, una vez más, la idea del aumento de actividad a nivel global. Una disminución de 9 millones de eventos en toda la red no puede justificar la pérdida de representatividad del Top-10 de 47 millones, casi la misma cantidad de eventos que registró el país con más presencia en la red de Aristeo.

ESTUDIO DE AMENAZAS POR INDICADOR

En colaboración con **Maltiverse**, hemos realizado un estudio clasificatorio de los indicadores de compromiso detectados en su plataforma. Esto es, indicar atributos interesantes sobre maliciosidad detectada en direcciones IP, nombres de dominio y URLs de los últimos seis meses.

En total, respecto a los diferentes IOCs involucrados se han estudiado: 261.447 direcciones IP, 62.740 dominios y 346.811 URLs.

¿Qué tipo de maliciosidad conllevan las URL estudiadas?

Como sabemos, las URL nos permiten acceder a recursos, describen un protocolo, una máquina en Internet (ya sea directamente a través de una IP o indirectamente desde un dominio) y dentro de esa máquina se especifica un recurso a través de una ruta.

Al final, en el contexto del malware, toda IP y dominio formará parte de una URL para solicitar un recurso. Ya sea una URL que nos dirige a un phishing y que posee un dominio muy parecido al original o puede ser que la URL sirva como punto de descarga de un malware.

Es importante determinar qué se encuentra al final de la URL y categorizarlo debidamente para saber a qué tipo de amenaza nos enfrentamos. Esto es precisamente lo que hemos

preguntado en la base de datos de Maltiverse y nos hemos encontrado con estos resultados en el top 10:

Malware Download	206081	59,99%
Phishing	129165	37,60%
Cobalt Strike	4148	1,21%
FAKEUPDATES	848	0,25%
GootLoader	759	0,22%
Coper	718	0,21%
DCRat	543	0,16%
Vidar	469	0,14%
Lumma Stealer	434	0,13%
Poseidon	387	0,11%

No hay sorpresas respecto a las dos categorizaciones con mayor número de indicadores: phishing y descarga de malware. Porque si hay un clásico en ciberseguridad respecto a que nos espera al final de una URL son precisamente estas dos grandes categorías.

No obstante, son categorías que agrupan o asimilan gran parte de lo que encontramos en la larga cola. El resto de las categorizaciones son más explícitas y nos indican incluso a que familia de malware pertenecen.

Por ejemplo, el ya clásico “Cobalt Strike” cuenta con un número récord dentro de su especialidad: más del 1% del total de URLs están relacionadas con este ejecutable que, aunque pertenece a una herramienta empleada en pentesting, la industria del malware ha sabido sacarle partido en sus operaciones.

¿Qué dominios son más empleados por las URLs marcadas como maliciosas?

Esta edición hemos efectuado consultas con Maltiverse para que nos diga cuáles son los dominios que aparecen con más frecuencia en las URLs estudiadas.

Es interesante observar qué servicios, legítimos en mayoría, son los más empleados por los creadores de malware y sus campañas asociadas.

Al final, una URL tendrá un alojamiento o redirección y necesita de un espacio o aplicación web ejecutable que en algún momento empleará para sus propósitos. Es el domino es que nos "chivará" dónde se ha alojado y de qué servicio ha hecho uso (ilegítimo).

pages.dev	14465	30,84%
workers.dev	7816	16,66%
github.io	5371	11,45%
r2.dev	4559	9,72%
weeblysite.com	3735	7,96%
cprapid.com	3136	6,69%
vercel.app	2512	5,35%
vacationstoremiamibeach.com	1791	3,82%
blogspot.com	1773	3,78%
wordbracer.shop	1752	3,73%

Muy interesante. "pages.dev" y "workers.dev" forman parte de un servicio "serverless" de Cloudflare. Al igual que casi todos los que aparecen en el ranking, son gratuitos hasta cierto punto. Los creadores de malware aprovechan las características de cuentas gratuitas para depositar su función y aprovecharlas hasta que son denunciados o descubiertos.

Abundan, como puede comprobarse y es norma, los sitios relacionados con el desarrollo o infraestructura de aplicaciones de carácter gratuito.

¿De qué países son las direcciones IP sobre las que se ha detectado actividad maliciosa?

Antes de contestar la pregunta, se ha de aclarar que porque un país aparezca en este ranking no significa que exista alevosía respecto de dicho país. Muchos países destacan sobre el resto por poseer más servicios y empresas de hosting lo que se traduce directamente en un mayor uso fraudulento. Un servidor puede estar alojado en un país y la organización criminal que haga uso de él puede proceder de otra nacionalidad.

Estados Unidos	44607	25,69%
India	39523	22,76%
China	35095	20,21%
Rusia	12509	7,20%

Alemania	8663	4,99%
Venezuela	8375	4,82%
Pakistan	6789	3,91%
Reino Unido	6518	3,75%
Brasil	6466	3,72%
Singapur	5114	2,94%

No existen grandes variaciones en este aspecto en los últimos años. Son países con grandes infraestructuras tecnológicas y, por lo tanto, como se ha comentado, proporcionalmente tienen un potencial mayor para ser usadas por el cibercrimen.

¿A qué tipo de maliciosidad se dedican las direcciones IP?

Mail Spammer	124717	71,82%
HTTP Spammer	107102	61,67%
Malicious host	54875	31,60%
SSH Attacker	34800	20,04%
Malware download	26485	15,25%
Proxy	25002	14,40%
Suspicious host	16205	9,33%
Bruteforce	13879	7,99%
HTTP Attacker	13479	7,76%
Port Scanner	13205	7,60%

Coronando el ranking del top 10 encontramos al indiscutible: el SPAM. Es la clasificación por antonomasia desde hace décadas ya. Y es que las reglas de marcado de SPAM son muy sensibles a esta actividad.

Prácticamente, podríamos decir que casi toda dirección IP pública habrá estado marcada como SPAM en algún momento.

El resto, salvando la categorización generalista de “Malicious host”, se divide de forma similar y repartida de forma casi ecuánime. Por ejemplo, y son actividades también clásicas, tenemos las direcciones IP que obran de proxies abiertos, ataques centrados en crear sesiones SSH (casi siempre: ataques por diccionario o fuerza bruta) o escaneo de puertos, sobre los que

entraría tanto los escáneres que realizan un censo de Internet como aquellos que poseen una actividad más inclinada a encontrar servicios abiertos y vulnerables.

¿Cuáles son los "top level domains" (TLD) con más dominios maliciosos?

Como sabemos, un dominio resuelve a una dirección IP. En el mundo del cibercrimen los dominios poseen una importancia capital dado que les permite hacer uso de este e ir cambiando la dirección de IP si el servidor en ese momento activo cesa su actividad maliciosa.

Un dominio se compone de varios niveles. Si nos fijamos son tramos de cadenas separados por puntos. Si obtenemos esos grupos de derecha a izquierda forman una jerarquía. El de más a la derecha es el dominio de nivel más alto.

Con ello, podemos agrupar los dominios categorizados como maliciosos por su dominio de nivel más alto. El resultado del top 10 es este:

com	16511	40,46%
dev	5997	14,70%
top	3613	8,85%
app	3350	8,21%
io	2782	6,82%
my.id	2292	5,62%
org	1852	4,54%
net	1578	3,87%
xyz	1438	3,52%
sn	1394	3,42%

No es sorpresa que los ".com" dominen el ranking, es el TLD con mayor número de dominios. Sin embargo sí que existen ciertos TLDs en la tabla que merecen una observación adicional, por ejemplo los TLD: ".app" y ".xyz". Además, tenemos nuevo huésped en el ranking con el dominio de nueva aparición "my.id" que consigue hasta desbancar a "biz" y "dev".

El TLD ".xyz" es muy usado en dominios maliciosos usados por el malware, en concreto y mucho, por los dominios generados aleatoriamente o mejor conocidos por su acrónimo: DGAs.

Respecto al ".app" es especialmente curioso ya que es un TLD por el que Google pagó más de 25 millones de dólares a la ICANN en febrero de 2015 para hacerse con su control. Además, es un TLD para el cual es obligatorio el tráfico HTTPS.

¿Qué categorización maliciosa poseen los dominios estudiados?

Los dominios están estrechamente ligados a las URL (del que forman parte) y también, por supuesto, de las direcciones IP a las que un dominio resuelve.

Veamos, por último, cómo se ha categorizado el top 10 de estos sobre los últimos seis meses.

Phishing	55113	92,06%
Malware download	1274	2,13%
Cobalt Strike	1003	1,68%
Cybergate	999	1,67%
CryptBot	387	0,65%
Poseidon	304	0,51%
Hydra	254	0,42%
AsyncRAT	200	0,33%
Lumma Stealer	167	0,28%
Hook	166	0,28%

Como ya hemos comentado, existe una relación muy estrecha entre dominios y URL y esto puede verse en el top 10 de categorías: phishing y malware.

CONCLUSIONES DEL INFORME

Si en 2023 las vulnerabilidades corregidas en iPhone han alcanzado su número más alto desde 2017, en la mitad de 2024 ya se han superado el número de ellas que permiten ejecución de código. En **Android, al contrario, parece que van por el camino de reducir las vulnerabilidades graves**. Si en 2023 fueron 32, en los seis primeros meses de 2024 solo cuentan con 12 críticas.

Con respecto al informe de transparencia de Apple, esta edición, **el gobierno alemán es el que más solicitudes ha generado para obtener información sobre dispositivos** desde que hacemos este seguimiento. Este liderazgo se extiende por primera vez, en el segundo semestre de 2022, al número concreto de dispositivos incluidos en las solicitudes. **Taiwán rebasa por primera vez a Estados Unidos en las solicitudes de información de cuentas por fraude en el segundo semestre de 2022**, España ocupa el cuarto lugar, aunque con un grado de aceptación por parte de Apple muy bajo (27%).Si Oracle, Microsoft y Google son las empresas con más fallos corregidos habitualmente, este semestre se cuela Linux, Adobe junto con Microsoft, dejando a Google y Oracle en el cuarto y sexto puesto respectivamente.

Con respecto a Aristeo, en el primer semestre de 2024 se detectaron **más de 313 millones de eventos de ciberseguridad**. Esto supone un pequeño descenso respecto a los datos registrados en el segundo semestre de 2023, 322 millones, y un ascenso respecto al segundo trimestre de 2023, cuando se registraron poco más de 300 millones de eventos. No obstante, las cifras se mantienen en rangos muy similares.

Algo muy curioso es una disminución notable de la actividad del Top-10 de países “sospechosos habituales” de ser origen de ataques. Pero este descenso refuerza la idea del aumento de actividad a nivel global. La respuesta es que, **aunque baja el número de eventos en los países más activos, esta actividad se ha trasladado a otros países tradicionalmente fuera de ese Top-10**, por lo que la actividad maliciosa queda más “repartida”.

Del análisis de los datos en Maltiverse, llama la atención la aparición de nuevos TLD entre los más usados para realizar actividades maliciosas: aparecen muy alto en el ránking "my.id" **que consigue hasta desbancar a "biz" y "dev".**

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.

CIBERSEGURIDAD

El error del billón de dólares
Microsoft Secure Future Iniciative (SFI): redoble de tambores
SSDLC: La clave para un software blindado
Ataque a la cadena de suministro en Linux: A fuego lento
23 and me o sobre cómo no gestionar un incidente de seguridad
Ciberseguridad y el golpe de los 10.000 millones de dólares

INTELIGENCIA ARTIFICIAL

Ataques a la Inteligencia Artificial (I): Jailbreak
Ataques a la Inteligencia Artificial (II): Model Poisoning
Ataques a la Inteligencia Artificial (III): Data Poisoning
Ataques a la Inteligencia Artificial (IV): Privacy Attacks
Inteligencia Artificial aplicada a la Ciberseguridad industrial (OT)
Evaluaciones de impacto de derechos fundamentales sobre sistemas de IA de alto riesgo en el RIA

MALWARE

Malware distribuido durante entrevistas de trabajo fraudulentas
Distribución de malware: ficheros en comentarios de GitHub
'Living off the land': cómo los atacantes emplean tus propias herramientas en su provecho