Telefónica Tech

Informe sobre el estado de la seguridad 2023 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.

Este primer semestre de 2023 se ha caracterizado entre otros muchos incidentes, por un fallo que ha dado bastante que hablar, por su presencia en grandes corporaciones precisamente para defender. El fallo, en FortiOS y FortiProxy con SSL-VPN habilitados de Fortigate, consiste en un problema de ejecución de código y el peligro es que los detalles de explotación se hicieron públicos el 13 de junio. Se conoce como CVE-2023-27997. Hasta aquí, es habitual ver este tipo de problemas graves de vez en cuando. En este caso llama la atención que, aunque lleva corregido desde el 8 de junio, todavía en julio existen 340.000 sistemas vulnerables. La industria sigue pendiente de ser más ágil parcheando sistemas críticos.

En la forma de atacar, hemos observado este semestre como se han vuelto a poner de moda ciertos ataques a través de la red de anuncios de Google durante todo el semestre. Esta técnica permite llegar a cualquier página con anuncios, legítima o no, para distribuir desde ahí anuncios que pueden contener malware. Se ha usado en campañas de ransomware y Google ha tenido que tomar cartas en el asunto para minimizar el problema. Este tipo de problemas de distribución de malware a través de anuncios fue un clásico de hace más de una década.

En febrero se observó una tendencia preocupante que parece que va al alza. La versión para Linux del ransomware Royal atacaba a servidores VMWare ESXi. Esto no es ya anecdótico. Desde 2022 se viene observando cómo el malware para sistemas Linux aumenta, tanto en su número como en sofisticación. Aunque nunca causen tanto ruido como el malware para Windows, es interesante ver la tendencia de los atacantes en este aspecto. El malware para Linux les permite por un lado atacar a infraestructuras que alojan máquinas virtuales, por ejemplo, en la nube, y secuestrar la base del sistema en vez de máquinas individuales. Por otro lado, los sistemas basados en Linux no suelen disponer de tantas herramientas de vigilancia incrustadas o incluso pueden encontrarse más desatendidos por los administradores en este aspecto. Es importante prestar atención a cualquier plataforma porque será el eslabón más débil por el que los atacantes quieran aprovecharse.

Por último destacar el problema que ha supuesto este año los adjuntos en formato OneNote, que habían pasado totalmente desapercibidos este año como vector de ataque. Desde comienzos de año han continuado los ataques en este formato y la industria, aunque tarde, ha sabido reaccionar hasta que son vigilados y detectados como cualquier otro formato. Los atacantes encontraron que este formato engañaba a los usuarios y les invitaba a abrir el fichero y ahí incrustaban de forma oculta ejecutables.

Este semestre, además de mantener nuestra sección especializada en el análisis de amenazas en el ámbito industrial gracias a nuestro proyecto **Aristeo**, contamos con **Maltiverse** como plataforma de consulta para analizar los principales IoC de la industria.

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 2023

A continuación, damos cuenta de aquellas noticias que mayor impacto han tenido durante el transcurso de este primer semestre de 2023.

ENERO

- **Nueva campaña de distribución de malware a través de anuncios de Google**. Los atacantes aprovechan la posibilidad de comprar anuncios y situarlos en las primeras posiciones de las búsquedas. Aunque Google los retira tras denuncia, se trata de un proceso manual y por tanto poco efectivo ante la repetición. Las principales razones del aumento del uso de este vector de ataque son un coste menor que el de los bots de spam, menores medidas de defensa implantadas en el proceso y la **capacidad de dirigir la campaña a un determinado grupo de usuarios**.
- El uso de los **gestores de contraseñas está en auge y eso conlleva una mayor atención por parte de los atacantes** ante este tipo de sistemas, lo vimos el año pasado con LastPass y se prevé una tendencia al alza en ataques a estos sistemas críticos. En esta ocasión se trata de Norton LifeLock que ha lanzado un comunicado de potencial compromiso de cuentas de usuario de su password manager. **La ironía, en este caso, es alta, el ataque se efectuó a través de *credential stuffing*** (reutilización de contraseñas encontradas en DarkWeb en otros servicios).
- **Microsoft anuncia que planea bloquear los archivos XLL provenientes de Internet en marzo**. En su lucha contra los archivos maliciosos bloqueará los archivos XLL provenientes de Internet, principalmente adjuntos en correos electrónicos. XLL es una extensión para complementos de Excel y básicamente un archivo DLL (bibliotecas de enlace dinámico). **No es habitual que este tipo de archivos se utilicen como adjuntos de correo electrónico, ya que suelen instalarlos los administradores. Sin embargo, dado que la extensión XLL está vinculada a un icono similar al de otras extensiones compatibles con Excel, las personas despistadas pueden confundirlas** con otros formatos de archivo de Excel.
- Un grupo de investigadores chino ha publicado un artículo científico donde aseguran que pueden (aunque no lo han hecho todavía) romper un cifrado RSA de 2048 bits usando computadores cuánticos. En este caso, expertos en criptografía no coinciden con la conclusión, pero la combinación de reducción de la base de celosía a través de la factorización con algoritmos de optimización cuántica puede ser una **amenaza real conforme la disponibilidad de la computación cuántica de mayor potencia vaya aumentando**.
- A partir del **5 de enero de este año los datos almacenados en servidores S3 de Amazon estarán cifrados por defecto**. Aunque esta opción estaba disponible desde 2011, se requería de una intervención por parte de los administradores para su activación.
- El 11 de enero, el grupo hacktivista "GhostSec" anunció que había conseguido ejecutar un ransomware en un dispositivo RTU ("Remote Terminal Unit") en una operación Bielorrusia. Este anuncio es muy relevante, ya que sería la primera vez que se consigue ejecutar este malware en un dispositivo tan limitado (y de uso tan frecuente en entornos industriales) como una RTU. El modelo concreto ha sido un "TELEOFIS RTU968 V2" y en los ficheros modificados se podían encontrar insultos contra el actual presidente de Rusia.

Varios grupos investigadores analizaron el caso y concluyeron que el vector de ataque pudo haber sido el servicio SHH que despliegan estos dispositivos, con una contraseña débil preconfigurada. También hicieron una búsqueda en un metabuscador y detectaron 117 dispositivos en la misma zona expuestos y con el servicio activado.

FEBRERO

- **Un estudio de Chainalysis sobre la industria del ransomware muestra un descenso en los pagos realizados en 2022 comparado con 2021**. ¿Qué significa esto y qué razones pueden justificar ese descenso? Probablemente esta reducción se deba a una combinación de factores entre los que destacamos dos: por economía de escala, como cualquier otro negocio, es muy complicado sostener las tasas de crecimiento que mostraba el ransomware en los últimos años y por otro lado**, los atacantes necesitan cada vez más ser un blanco móvil ante una mayor vigilancia**, por lo que se reorganizan con mayor rapidez y son menos duraderas (de 1 año a 2 meses de vida) esto también puede afectar a su capacidad de impacto.
- **Bélgica** se une a un listado cada vez mayor de países que lanzan **programas de notificación de vulnerabilidades nacionales, con el objetivo de proteger a los investigadores que buscan vulnerabilidades**, pero no tienen planeado ningún uso malicioso de las mismas. Bélgica se une así a Holanda, Francia y Lituania dentro de Europa.
- Record DDoS: Cloudflare ha comunicado que ha mitigado este febrero el **mayor ataque de denegación de servicio distribuido hasta la fecha, con más de 71 millones de peticiones HTTPS por segundo**. Un dato un 35% más alto que el anterior ataque registrado en el ranking con 46 millones de *rps* (requests per second).
- En los dispositivos **IoT la seguridad no suele ser una prioridad.** Este mes hemos visto varios ejemplos que tratan de avanzar en la provisión de recursos para el sector IoT: el instituto de estándares y tecnologías americano (NIST) ha anunciado un grupo de algoritmos criptográficos ligeros (Ascon) se convertirá en estándar en 2023, Microsoft ha abierto el código de CHERIoT un sistema operativo de tiempo real que sigue el precepto de *security-first*.
- La **Audiencia Nacional** ha accedido finalmente a la solicitud de las autoridades de Estados Unidos para que **extradite** a un joven británico de 23 años que supuestamente participó en el famoso **hackeo, en julio de 2020, de numerosas cuentas de Twitter como las de Joseph Biden, Barack Obama o Bill Gates**.
- **El crecimiento exponencial en popularidad de chatGPT atrae a los distribuidores de *malware*. Estos tratan de aprovechar el hype para garantizar la repercusión de sus ataques**. Los Investigadores de Kaspersky han detectado una falsa versión de escritorio para Windows de ChatGPT empleada para la distribución de *malware*.
- El 22 de febrero, la empresa Dole food company, especializada en el cultivo y distribución de frutas y verduras, anunció que había sido afectada por un ataque con ransomware. El ataque interrumpió las operaciones de la empresa, provocando el cierre temporal de sus plantas de embalaje y distribución y, por lo tanto, cortando el suministro a las tiendas de los EE.UU. Además de la paralización de las operaciones, principalmente en sus plantas chilenas, los atacantes también se llevaron información de la empresa, incluyendo datos de ciertos empleados. El 18 mayo, Dole presentó su informe económico del primer trimestre y cuantificó en 10.5 millones de dólares los costes de este ataque.

MARZO

- La base de datos de vulnerabilidades cuya explotación es conocida (KEV Database) de la agencia de ciberseguridad e infraestructura americana (CISA) casi se ha triplicado, pasando de 311 a 868 registros a final de 2022. Un estudio de VulnCheck revela que la gran mayoría de las nuevas entradas no son por vulnerabilidades nuevas, sino que más del 80% son vulnerabilidades antiguas, de hecho la más antigua es de 2002.
- **Github ha introducido para todos sus usuarios una funcionalidad que permite escanear los repositorios de código en busca de secretos que pudiesen haber sido incorporados de forma accidental**. La funcionalidad se puede lanzar desde el propio perfil de usuario de Github y suporta más de 100 formatos de API tokens.
- La compañía de ciberseguridad Netscout ha publicado un análisis donde se puede comprobar la **efectividad de la eliminación de más servicios de alquiler de ataques DDoS**. **La eliminación a finales de 2022, en una acción conjunta de Europol y el FBI, de más de 50 servicios de DDoS ha resultado en un significativamente menor número de ataques**. Además, la continuidad de esta tendencia transcurridos tres meses denota la ausencia de nuevos actores importantes en este sector.
- El proveedor de software de Voz sobre IP 3CX fue comprometido para lanzar un ataque de gran escala de cadena de suministro. A pesar de que 3CX cuenta con más de 600.000 clientes, **dos factores influyeron en que el impacto no fuese enorme**. Por un lado, la **detección fue muy rápida (semanas) desde la activación**, por contexto en SolarWinds se tardó nueve meses. Por otro lado, se trataba de un **ataque altamente dirigido, a compañías en el ámbito de las criptomonedas** y no generalista.
- Microsoft ha anunciado que planea **bloquear de forma progresiva y previo aviso aquellos correos que provengan de servidores Exchange "on premises" que no estén correctamente parcheados y sean "persistentemente vulnerables"**.

ABRIL

- **Samung ChatGPT leak**: con la aparición de la inteligencia artificial generativa, muchos **empleados se han visto seducidos por la capacidad de aceleración que estos sistemas pueden proporcionar y no han pensado las potenciales implicaciones de privacidad que puede implicar su uso**. En concreto, Samsung notificó este abril a sus empleados que limitasen el uso de chatGPT después de detectar la publicación de documentos y código fuente internos y restringidos para la detección de chips defectuosos.
- En marzo hablábamos de la base de datos KEV (Known Exploited Vulnerabilities) de la agencia americana CISA, pues la compañía *Rezilion* ha escaneado internet buscando sistemas expuestos a las más de 800 vulnerabilidades descritas en la base de datos y los resultados no son buenos. **Se han detectado más de 15 millones de sistemas a nivel global que necesitarían parcheados para evitar un ataque sencillo**. Las dos vulnerabilidades de más exposición son, de forma lógica, asociadas con servidores Web (en concreto Apache), pero podemos encontrar datos sorprendentes

como los **casi 200.000 sistemas expuestos a Heartbleed cuyo descubrimiento cumple casi 10 años**.

- **El *lockdown mode* lanzado por Apple a mediados de 2022 se apunta sus primeros éxitos al detener un ataque 0-day**, proveniente del grupo NSO según refleja *Citizens Lab* en su análisis, que no requería ninguna interacción del usuario, a un dispositivo iOS con la funcionalidad activada. Incluso se notificó a la víctima del intento de explotación en su terminal en el momento de la activación.
- No es común pero a veces sucede, **HP ha tenido que avisar a los clientes de algunas impresoras láser que hagan un *downgrade* del firmware de sus impresoras**, ya que la última actualización, introdujo una vulnerabilidad de exposición de información que no han logrado parchear todavía. Estiman que puedan lanzar una nueva versión parcheada en los próximos 90 días.
- Los troyanos de suscripción para Android continúan haciendo daño a raíz de un estudio de Kaspersky. En esta ocasión se trata de una familia de troyanos conocida como *Fleckpe*. **El código malicioso se esconde en aplicaciones de edición de fotos o fondos de escritorio y actúa de forma silenciosa abriendo un navegador en modo oculto para suscribir a las víctimas a servicios premium**, si se requiere la confirmación con un código la aplicación previamente solicita el acceso a notificaciones y las lee automáticamente sin interacción del usuario. La *app* posteriormente funciona con normalidad aumentando las posibilidades del ataque de pasar desapercibido durante un mayor tiempo.
- Investigadores de Bitsight y Curesec han descubierto que el **protocolo SLP** (Service Location Protocol) usado desde 1997 por impresoras, ordenadores, routers, etc para facilitar el descubrimiento de servicios **puede ser usado en ataques DDoS por su alto factor de amplificación en un factor de más de 2200, el tercer factor de amplificación más alto conocido hasta la fecha**. Este protocolo está más orientado a uso en LAN pero muchas veces se encuentra expuesto a internet ya que viene en las versiones estándar de HW y SW. Más de 70000 servidores tienen los puertos SLP expuestos al exterior en base al estudio realizado.
- Todos los meses de abril, desde hace unos 10 años, se activa la operación "OPIsrael". El 5 de abril, el servicio de correos de Israel tuvo que cerrar algunos servicios por un ciberataque. Dos días después, los controladores de agua del valle del Jordán estaban bloqueados y mostraban un mensaje contra Israel. Otras acciones, menos sofisticadas, implican ataques contra sitios web de universidades, servicios de transporte, gobierno...

MAYO

- Las ***Rapid Security Responses* son un nuevo mecanismo que se han puesto en marcha en los sistemas Mac y que se asemeja a los parches fuera de ciclo de Windows**. Tratan de **acelerar la mitigación de *zero-days* críticos y otras mejoras de seguridad urgentes**. De esta forma, se agiliza la respuesta y la instalación es más rápida al no tener que realizar una actualización completa del sistema. Se identificarán con una letra tras la versión por ejemplo iOS 13.3.1 pasaría a ser iOS 13.3.1(a).
- Automattic, la empresa detrás del producto Wordpress.com, o sea, del servicio de alojamiento. **Ha forzado la actualización a millones de webs que usan el plugin Jetpack**. Jetpack, es uno de los plugins que mantiene y que se instala casi por defecto en cada Wordpress, precisamente porque

previene ataques fuerza bruta, hace backups, etc. Tiene más de 5 millones de instalaciones activas y en el momento de la publicación no se conocían ataques activos a la **vulnerabilidad, encontrada mediante una auditoría interna, en su API desde la versión 2.0 (2012) y que permitiría a los autores de un sitio a modificar cualquier fichero de la instalación de Wordpress**.

- **El nuevo TLD (*Top Level Domain*) .zip lanzado por Google ha generado mucha controversia en el ámbito de la ciberseguridad** ya que muchos expertos coinciden en que puede **desencadenar nuevos ataques por la familiaridad de los usuarios con este tipo de ficheros comprimidos**. Por ejemplo, usando el buscador del explorador de archivos de Windows si un usuario busca ejemplo.zip y no se encuentra lo abrirá automáticamente en un navegador que llegará a este nuevo TLD.
- *Scalper bots* es la denominación que tienen las herramientas que tratan de automatizar el rápido consumo de un recurso escaso en internet para posteriormente vender el acceso a ese recurso a víctimas por un precio mayor o por un coste cuando era gratuito. Por ejemplo, los fraudes en las entradas a conciertos, etc. En mayo se ha **desmantelado una red de bots en España que se dedicaban a reservar todas las citas previas para peticiones de asilo. Posteriormente vendían las reservas de citas a extranjeros que necesitaban esos servicios por un precio entre los 20 a los 300 euros cuando en realidad es un servicio gratuito**. Se han detenido 70 personas relacionadas con la trama.
- Académicos de la universidad de Maryland han descubierto que algunos **dispositivos requisados por las autoridades americanas y no reclamados por sus dueños originales son subastados sin haberlos devuelto a su estado de fábrica ni limpiado los datos de los terminales**. Esto expone a los citados dueños a posibles crímenes de extorsión o filtración de información sensible. De las 228 unidades requisadas por la policía y compradas por los investigadores a través de la web PropertyRoom.com, **pudieron extraer mensajes de redes sociales, documentos identificativos, cuentas y tarjetas bancarias** e incluso videos y fotografías con contenido sexual explicito.
- **La utopía del mundo sin contraseñas parece algo más cerca** tras el anuncio de Google de introducir el soporte a las *passkeys* para las cuentas personales. **Con un *passkey* puedes acceder a tu cuenta de Google autenticándote en un dispositivo local por ejemplo través de biometría**.
- Mandiant identifica un nuevo malware, denominado “CosmicEnergy” diseñado para interrumpir el suministro eléctrico al interactuar contra RTU y sistemas de comunicación basados en el estándar IEC-104. Este tipo de dispositivos son de uso común en Europa, Oriente medio y Asia. El análisis revela capacidades comparables con el malware Industroyer, que generó graves problemas en Kiev en 2016. La investigación de este equipo encontró una traza de un proyecto llamado “Solar Polygon”, que fue un proyecto desarrollado por Rostecom-Solar, una empresa rusa de ciberseguridad que recibió una ayuda del gobierno ruso en 2019 para ejecutar ejercicios de capacitación y de respuesta ante incidentes. Cómo habría acabado este malware fuera de su uso legítimo es un misterio.

JUNIO

- Investigadores de TrendMicro advierten de la potencia del **motor de ofuscación de malware llamado *BatCloak* que prácticamente convierte al código malicioso**, a raíz de los datos obtenidos de las más de 750 muestras, **en indetectado** (FUD: fully undetectable malware). El 80% de las muestras obtenidas por los investigadores en 2022 no son detectadas por ningún motor de antivirus. Esto proporciona un escenario ideal para los atacantes para incorporar malware a través de ficheros batch procesados por *BatCloak*.
- **Toyota** ha comunicado que ha encontrado nuevos servidores expuestos con información de clientes desde 2015 y 2016 respectivamente, esta noticia aviva la llama, ya que viene tras la notificación del descubrimiento en el mes de mayo de una **base de datos expuesta con información de los clientes de Japón durante casi 12 años**.
- OWASP ha publicado un borrador de los **Top10 riesgos** de seguridad asociados con el trabajo con **aplicaciones basadas en grandes modelos de lenguaje (LLMs)**, El riesgo más elevado son las vulnerabilidades de *prompt inyection* que permiten a través de sofisticadas manipulaciones de la entrada causar un efecto inesperado como la revelación de información o acciones no autorizadas o prevista en el diseño de la aplicación.
- Microsoft atribuye al grupo de cibercrimen **Clop como el autor del ataque a los servidores MOVEit** de la empresa Progress Software. Se han detectado ya más de 100 empresas afectadas por el robo de información o extorsión tras aprovechar la vulnerabilidad zero-day de inyección SQL (CVE-2023-34362). **El ataque denota una gran profesionalización con más de 2 meses de fase de preparación y un ataque en víspera de puente en Estados Unidos el país con mayor número de activos**. Censys muestra entre 2500 y 3000 servidores MOVEit expuestos en internet por lo lamentablemente parece que la división de extorsión de la banda criminal va a tener mucho trabajo.
- Freaky Leaky SMS: Un equipo de académicos ha descubierto una nueva técnica que puede permitir a un atacante determinar la localización de un usuario de teléfono móvil con alta precisión. **El ataque, del tipo *timing attack*, consiste en el envío de varios mensajes SMS y la medición de los tiempos entre los envíos y la entrega de los SMS delivery reports que genera de forma automática la telco que da servicio a la víctima**. Los autores llegan a obtener un 96% de precisión en algunos escenarios.
- Por fin, **Microsoft va a cambiar la configuración por defecto de SMB para que las peticiones vayan firmadas**. A pesar de que esta opción existía desde Windows 98 no se establecía por defecto ya que ralentiza las transferencias de información. Sin dicho firmado, se podían ejecutar lugar a ataques "*relay NTLM*".
- El 3 de mayo, Dallas, una de las 10 ciudades más pobladas de los EE.UU, se vio afectada por un ransomware que dejó interrumpió los principales servicios de la ciudad. Un mes más tarde, el 9 de junio, los funcionarios de la ciudad anunciaron que habían conseguido avanzar en la restauración de estos sistemas hasta el 90%, aunque aún quedaba mucho por hacer. El ataque del ransomware Royal dejó fuera de servicio bibliotecas, refugios de animales, departamentos de seguridad y otros servicios gubernamentales, sistemas de pago online, medidores de caudal de agua... Además, los atacantes se hicieron con información que más tarde amenazaron por divulgar si no recibían un pago como contraprestación.

MÓVILES

Apple iOS

Nuevas características de seguridad

Apple anunció el 5 de junio nuevas medidas en el apartado de seguridad y privacidad. Entre ellas, comentamos las más destacables.

Una de las medidas se trata de un modo de bloqueo en la navegación privada de Safari, que permitirá bloquear el navegador si no se ha usado el navegador nativo de Apple en un espacio determinado de tiempo. Con ello se quiere impedir que alguien con acceso al dispositivo pueda ver qué pestañas se mantenían activas en dicho modo.

Se ha mejorado la selección de fotos a compartir con las aplicaciones presentando un diálogo con más opciones al respecto.

También se ha mejorado un aspecto muy de moda ahora como es el seguimiento de usuarios a través de parámetros en las URLs. En algunas webs, los usuarios son seguidos vía parámetros personalizados que identifican unívocamente a cada usuario, Apple ha mejorado la detección y filtrado de dichos parámetros, dificultando su uso.

Adicionalmente, va a implementar un mecanismo de aviso de contenido explicito en material compartido a través de mensajes. Este mecanismo suscitó cierta polémica (de hecho, se detuvo su puesta en marcha) dado que no estaba claro cómo se estaba implementando. Esperemos tener más detalles acerca del funcionamiento de esta característica.

Otra característica es la de compartición de contraseñas entre contactos conocidos y autorizados desde un dispositivo. La idea es más la posesión de contraseñas que todos pueden ver, usar y cambiar. Una característica que soluciona ciertos problemas de usabilidad pero que está por ver como se desenvuelve, desde el punto de vista de la seguridad, en un uso real.

Por último, algo curioso. Si se ha cambiado la contraseña se acceso a un dispositivo con iOS, se mantendrá un periodo de gracia de 72 horas en el que aun seguirá siendo válida la antigua contraseña. Sin duda una medida que quizás viene del alto porcentaje de usuarios que olvidan la nueva contraseña de acceso.

Vulnerabilidades y nuevas versiones

Repasamos las actualizaciones de seguridad del sistema operativo iOS que nos ha traído el primer semestre de 2023.

iOS 16.3

Nos encontramos en enero, venimos de un iOS 16.2 y con un mes de diferencia Apple libera la tercera revisión de la rama actual de su sistema operativo para móviles. El 23 del primer mes de 2023 ve la luz iOS 16.3. En esta ocasión viene con un lote de 17 CVE o vulnerabilidades parcheadas de diversa consideración.

De entre las 17, revierten cierto peligro las correspondientes al motor de renderizado HTML Webkit, tres en concreto, que podrían permitir la ejecución de código arbitrario con tan solo visitar una página web malintencionada.

iOS 15.7.3 y 12.5.7

Ese mismo día de enero es publicada la versión 15.7.3, un patch level que corrige cinco vulnerabilidades, ninguna que permita ejecución de código arbitrario, pero sí una elevación de privilegios a nivel de kernel.

Además, también se publica un parche (CVE-2022-42856) en la versión 12.5.7 que permite ejecución de código arbitrario en WebKit o lo que es lo mismo: al visitar una web malintencionada con Safari. Apple confirma que el fallo está siendo explotado activamente y en especial, en versiones inferiores o anteriores a la 15.1.

iOS 16.3.1

13 de febrero, grupo de tres parches, uno de especial interés. Al igual que el comentado anteriormente para 12.5.7, tenemos un nuevo fallo afectando a Webkit que posibilita la ejecución de código arbitrario con solo visitar una web maliciosa. Tiene el CVE-2023-23529. Además, Apple confirma igualmente que está siendo activamente explotado.

iOS 16.4

Casi acabamos marzo sin ninguna actualización, pero el 27 de dicho mes se libera la nueva versión de iOS 16, la 16.4. Además, lo hace con una larga lista de correcciones de seguridad. Nada más y nada menos que 37 parches. Aunque solo una permita la ejecución remota de código arbitrario, llama la atención la gran cantidad de fallos relativos a la evasión de medidas de protección de los datos considerados personales o privados por parte de aplicaciones malintencionadas.

iOS 15.7.4

El mismo día de la liberación de iOS 16.4 la rama aun mantenida, iOS 15.7, recibe su cuarta iteración esta vez con un lote de 19 parches, cuatro de ellos corrigiendo fallos que podrían derivar en ejecución de código arbitrario de forma remota. También incluye el parche para iOS 15 del arriba comentado CVE-2023-23529.

16.4.1 y 15.7.5

De nuevo, un parche urgente y de nuevo afectando a WebKit (motor de renderizado de Safari), para variar activamente explotado. Este parche corrige dos vulnerabilidades incluyendo la comentada. Su matrícula es el CVE-2023-28205.

Curiosamente, se libera para iOS 16.4.1 el 7 de abril y tres días más tarde, el 10 de abril lo hace para la versión 15.7.

16.5 y 15.7.6

Estamos a 18 de mayo y en el mismo día liberan la quinta iteración de la rama 16, que llega a su ecuador y la sexta para la 15.7.

Para la 16, son confirmados 38 parches con cinco de ellos con correcciones de especial peligrosidad ya que los fallos permitían la ejecución remota de código arbitrario e incluso algunos de ellos activamente explotados.

Para 15.7 son corregidas 16 vulnerabilidades, tres de ellas con fallos de ejecución remota de código arbitrario.

16.5.1 y 15.7.7

Cerramos el semestre con un nuevo susto. Parche de urgencia que cubre dos fallos graves en iOS 16.5. El CVE-2023-32439 afectando a WebKit (Safari) y el otro, CVE-2023-32434, al kernel. Ambos activamente explotados.

Para 15.7, la séptima revisión, y también de urgencia, tapa los comentados fallos anteriores más uno adicional para WebKit que también ha sido visto activamente explotado. Su matrícula es el CVE-2023-32435.

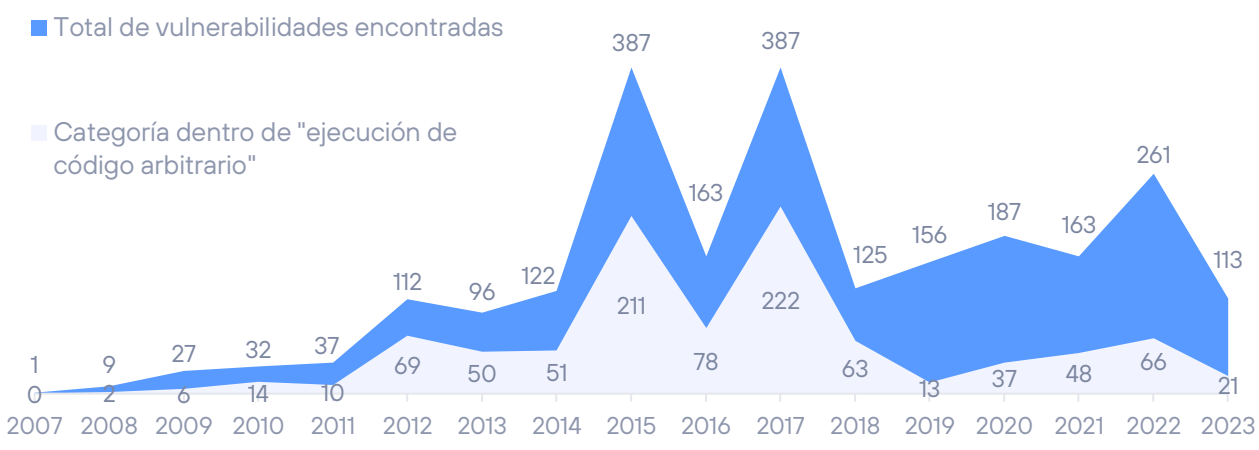
Evolución de vulnerabilidades en iOS durante el primer semestre de 2023

El primer semestre de 2023 se ha cerrado con 113 vulnerabilidades únicas parcheadas, alrededor de la docena consideradas de alto riesgo, con posibilidad de ejecutar código arbitrario. Algunas de ellas afectando al propio núcleo del sistema operativo.

Si se mantiene la tónica es posible que veamos un año similar en números a 2022

VULNERABILIDADES EN IOS 2023-H1

Evolución de vulnerabilidades por año



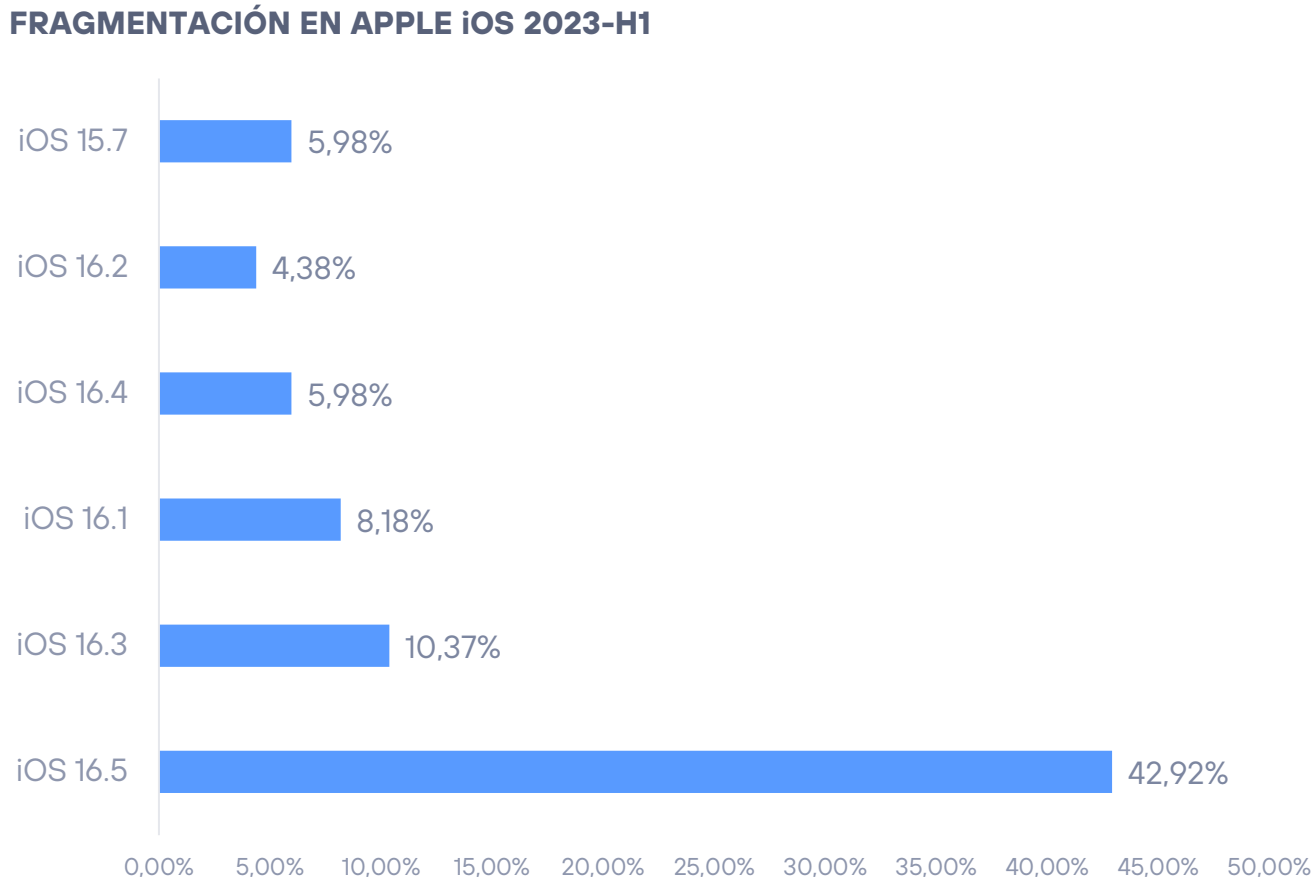
Fragmentación de versiones durante el primer semestre de 2023

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, tenemos a iOS 16 en la mitad de su vida útil (siempre y cuando Apple continue con el mismo ritmo de salida de nuevas versiones).

Actualmente, la rama 16 copa en absoluto la tarta del reparto de versiones de iOS:



Tan solo obtiene una representación mínima iOS 15.7 que se resiste a cambiar con un 5.98% del share.

Informe de Transparencia de Apple

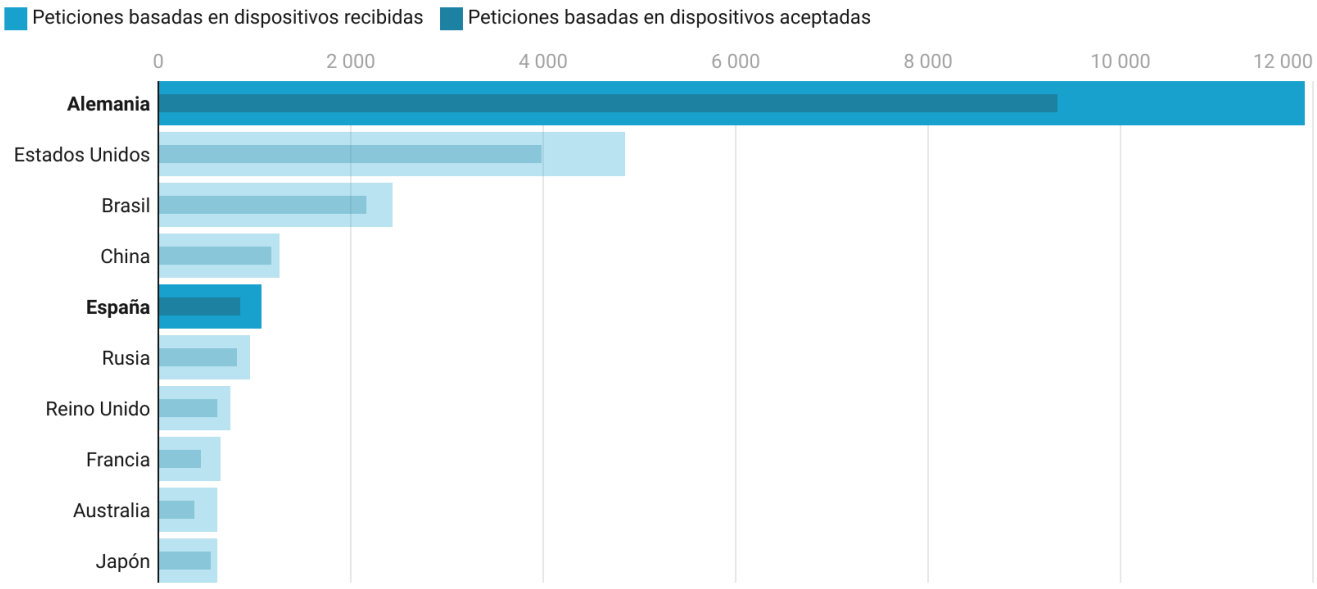
En ocasiones, los gobiernos necesitan apoyarse en las grandes corporaciones para poder llevar a cabo su trabajo. Cuando una amenaza pasa por conocer la identidad o tener acceso a los datos de un potencial atacante o de una víctima en peligro, la información digital que almacenan estas empresas puede 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 2021 (el último publicado por Apple a fecha del primer semestre de 2023)** 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.

Alemania es el país que más solicitudes de información de dispositivos ha realizado en el segundo semestre de 2021

Se muestran el número total de peticiones realizadas y aquellas que han sido aceptadas por Apple.



Dentro de este Top10 el grado de aceptación varía desde el 62% para las peticiones de Australia al 93% para las correspondientes a China.

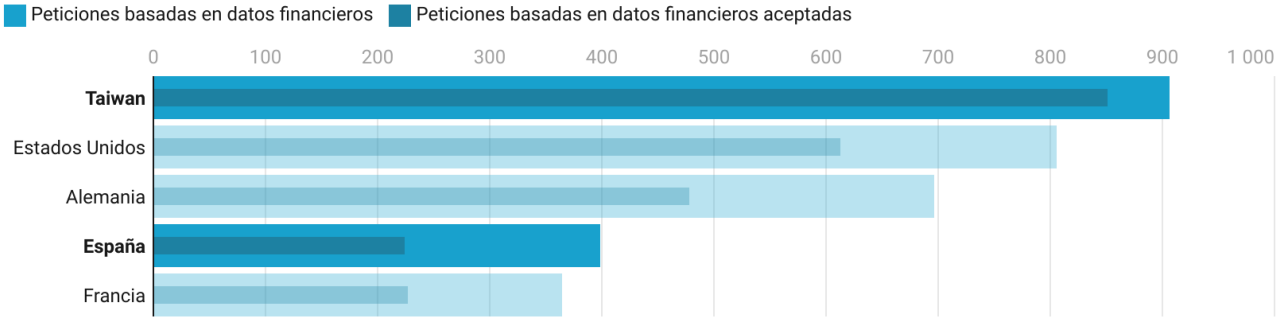
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

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.

Taiwan lidera las solicitudes de información por fraude en el segundo semestre de 2021. España ocupa el cuarto lugar en número de solicitudes.

Se muestran el número total de peticiones realizadas y aquellas que han sido aceptadas por Apple.



El grado de aceptación entre los 5 paises con mayor volúmen varía desde el 56% para las peticiones precisamente de España al 94% para las correspondientes a Taiwan.

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...).

EEUU es, con diferencia, el país que más solicitudes de información de cuenta ha realizado en el segundo semestre de 2021

Se muestran el número total de peticiones realizadas y aquellas que han sido aceptadas por Apple.

De las 84 peticiones realizadas por España en los seis últimos meses de 2021 47 fueron aceptadas (56%).

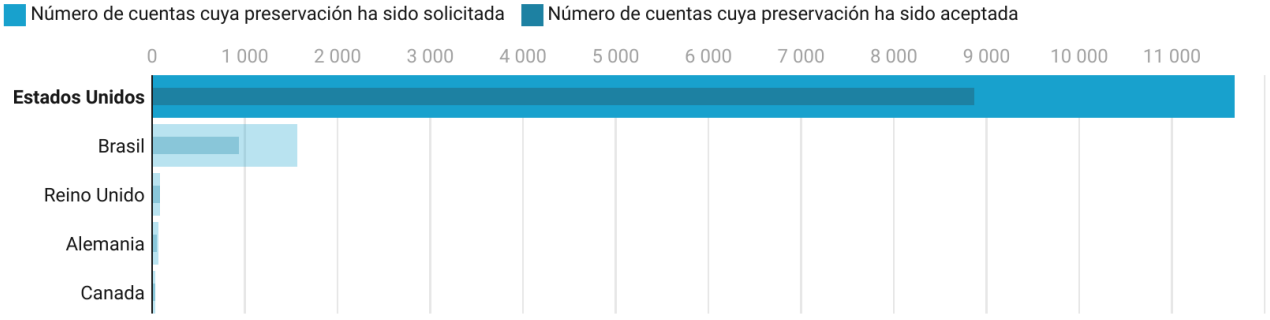
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

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 es el país que más cuentas ha solicitado preservar en los segundos seis meses de 2021

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 este periodo.

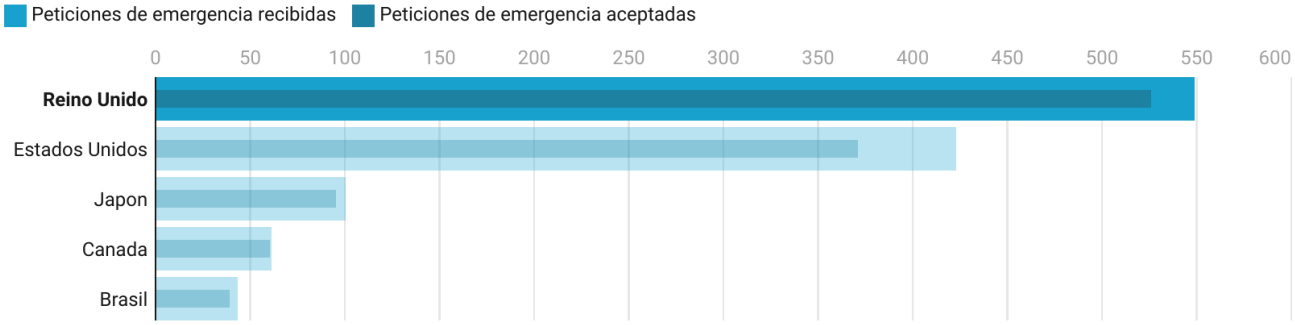
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

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 es el país que más peticiones de acceso a cuentas por emergencia solicita en el segundo semestre de 2021.

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



España, que ocupa el puesto 29 en el ranking, solamente emitió 1 solicitud de acceso a cuenta por emergencias y fue aceptada (100%).

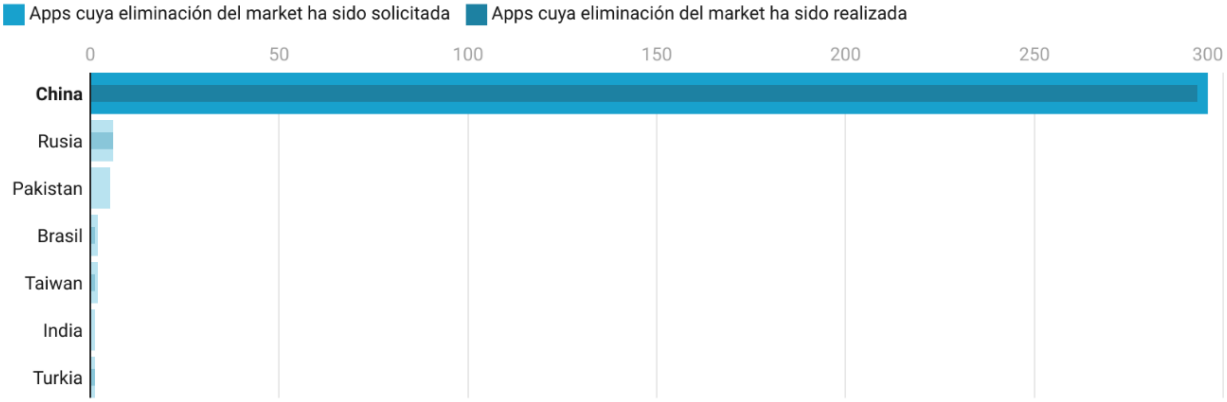
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

Peticiones relacionadas con la retirada de apps del market

Habitualmente tiene que ver con aplicaciones que se supone violan la ley soberana del país/región solicitante.

China solicitó 296 eliminaciones de Apps del market en los segundos seis meses de 2021, siendo el 99% de las apps eliminadas por Apple.

Se muestran las Apps cuya retirada del respectivo market ha sido solicitada y aquellas Apps efectivamente eliminadas.



Esta cifra triplica las eliminaciones solicitadas por China en los primeros seis meses del 2021.

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.
- **Taiwan ha duplicado las solicitudes de información de cuentas por fraude** que ha realizado en 2021, pasando de las 1.000 solicitudes de 2020 a las más de 2.000 en 2021.
- 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 destaca de nuestro análisis es que **Brasil está en segundo lugar de una forma muy destacada con 10 veces más solicitudes de preservación y acceso 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 EEUU. Esto refuerza la teoría de que exista un procedimiento de lanzamiento de este tipo de solicitudes por parte de su departamento de exteriores.
- De manera poco sorprendente, China continúa siendo el país que más retirada de *apps* solicita en el App Store. La diferencia es enorme con el resto del mundo, de las casi **300 *apps* cuya eliminación ha sido solicitada por China** en el último semestre de 2021 **pasamos a solamente 6 para Rusia** que ocupa la segunda plaza en este listado.

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

Android 14 está a punto de salir del horno de Google puesto que nos acercamos ya a la fecha de aniversario de Android 13, precisamente, el 13 de agosto. La versión 14 se conoce internamente como "Upside down cake".

La primera medida de seguridad en el nuevo Android será bastante curiosa: impedir la instalación de aplicaciones para versiones de Android 5.1 y anteriores. Es decir, hasta 14, se permitía la instalación de aplicaciones con, literalmente, años, incluido un buen catálogo de malware procedente de un ya lejano pasado.

Android 14 implementará por fin una selección más granular de que archivos podemos compartir con una aplicación determinada. Una característica muy inspirada a la que ya ofrece iOS desde hace bastantes versiones.

Se da un paso también a la integración de "Passkey" en "Credential Manager" permitiendo a los usuarios disfrutar de una experiencia más integrada y fluida de este método de autenticación alternativo a las contraseñas y muy centrado en la posesión del dispositivo.

Un paso más en conectividad: Android 14 soportará comunicaciones satelitales. Si el chip lo soporta, permitirá a los usuarios conectarse y realizar llamadas (por ejemplo, e importante: de emergencia) si no tenemos conexión con antenas de telefonía, pero sí satelital.

Queda poco para que se haga oficial Android 14, veremos que nuevas características nos trae cuando sea oficialmente liberado.

Vulnerabilidades

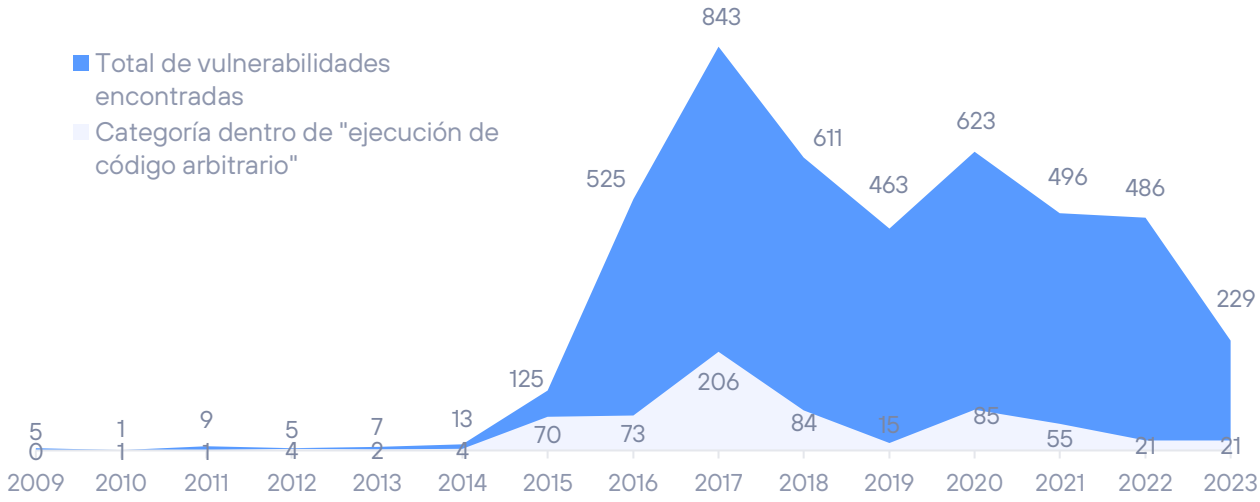
Android publica un conjunto de parches cada mes, generalmente durante la primera semana. En este primer semestre de 2023 se han publicado seis boletines con una distribución de 33, 35, 39, 43, 38, 41 parches o CVE corregidos. Igualmente, por aparición, los fallos críticos se distribuyen en 1, 2, 3, 9, 1, 5 respectivamente.

En total, 229 parches (el semestre anterior fue de 256); 21 de ellos considerados críticos (14 en el semestre 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 2023-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 10, con un share del 23.33%, seguida por la 13 con un share de 22.38%.

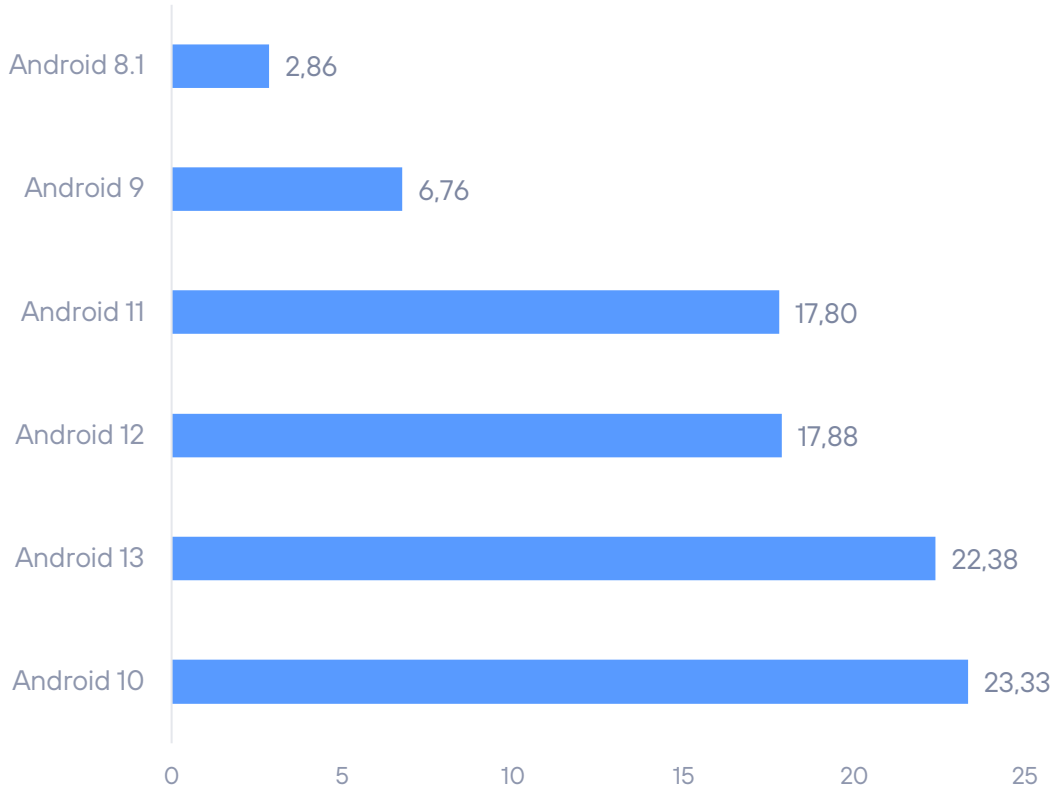
Es típico en Android que las nuevas versiones del sistema operativo tarden bastante en ser adoptadas debido sobre todo a que cada fabricante debe personalizar y adaptar los cambios a las particularidades del dispositivo e idiosincrasia de la marca.

La nueva versión, Android 13, que tan solo estaba disponible en un 6.72% en el semestre anterior consigue auparse al segundo puesto, pero sorprende no obstante que la versión 10 aun tenga tirón y remonte posiciones. Puede ser debido a la fragmentación de versiones inferiores a la 13 o a un cambio en la metodología de medición del proveedor.

La porción restante se la reparten las versiones 12 con un 17.88%, y 11 con un 17.8%.

Sigue siendo alarmante que Android 9.0 y 8.1 aun poseen una cuota conjunta de un 9.62% algo menos del 14% que arrojaban el semestre anterior. Como ya comentamos, es un peligro que estas unidades aun estén en funcionamiento y con un parqué de dispositivos tan significativo. No reciben actualizaciones de seguridad y poseen software potencialmente vulnerable. Un auténtico riesgo.

FRAGMENTACIÓN EN ANDROID 2023-H1



VULNERABILIDADES DESTACABLES

Comentamos en esta sección algunas de las vulnerabilidades notables a nuestro juicio, de este primer semestre de 2023, es decir, aquellas que destacan por su especial relevancia o peligrosidad.

CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2023-20076	Cisco IOx application hosting	Una vulnerabilidad en el espacio de aplicaciones IOx, que se basa en una incorrecta sanitización de parámetros, puede permitir que un atacante remoto (autenticado) ejecute comandos como root e incluso pueda implementar y activar una aplicación en este entorno con un fichero de carga modificado.	8.8
CVE-2023-27997	FortiOS y FortiProxy de Fortigate	Ejecución de código en dispositivos con SSL-VPN habilitados de Fortigate.	9.8

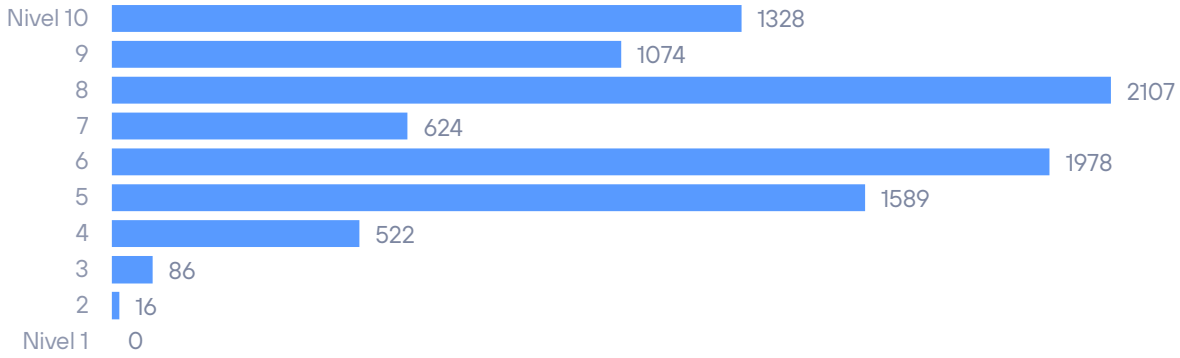
CVE-2023-22601	InHand Networks routers, InRouter 302 y 615	Dos routers de InHand, enfocados a su uso en entornos industriales, afectados por una capacidad insuficiente de generación de valores aleatorios al calcular el ID del cliente en el establecimiento de conexiones MQTT. Esto podría provocar que un atacante pudiera calcular este ID y obtener información de otros dispositivos conectados a la misma plataforma.	8.6
CVE-2023-32347	Teltonika's Remote Management System	El sistema de gestión remota de Teltonika (versión 4.10.0) sólo utiliza la MAC de los dispositivos y sus números de serie para para autenticarlos durante el acceso al sistema. Esto implica que alguien que conozca estos dos parámetros podría identificarse como uno de esos dispositivos y robar las credenciales del dispositivo, así como ejecutar código como root utilizando el panel de opciones del dispositivo legítimo.	9.8
CVE-2023-1424	Mitsubishi Electric Corporation MELSEC iQ-F Series	Versiones de estos dispositivos de campo son vulnerables a ataques de DoS y a ejecuciones de código malicioso a través de buffer overflow. Para la ejecución de código, el atacante debe conocer la estructura interna de los productos.	9.8
CVE-2023-21716	Microsoft Word	Fallo en wwlib de Microsoft Office, permite a los atacantes lograr la ejecución remota de código con los privilegios de la víctima que abre un documento RTF malicioso.	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. El número de vulnerabilidades en general se ha disparado con respecto al primer semestre.

RIESGO DE VULNERABILIDADES

Distribución de vulnerabilidades por riesgo

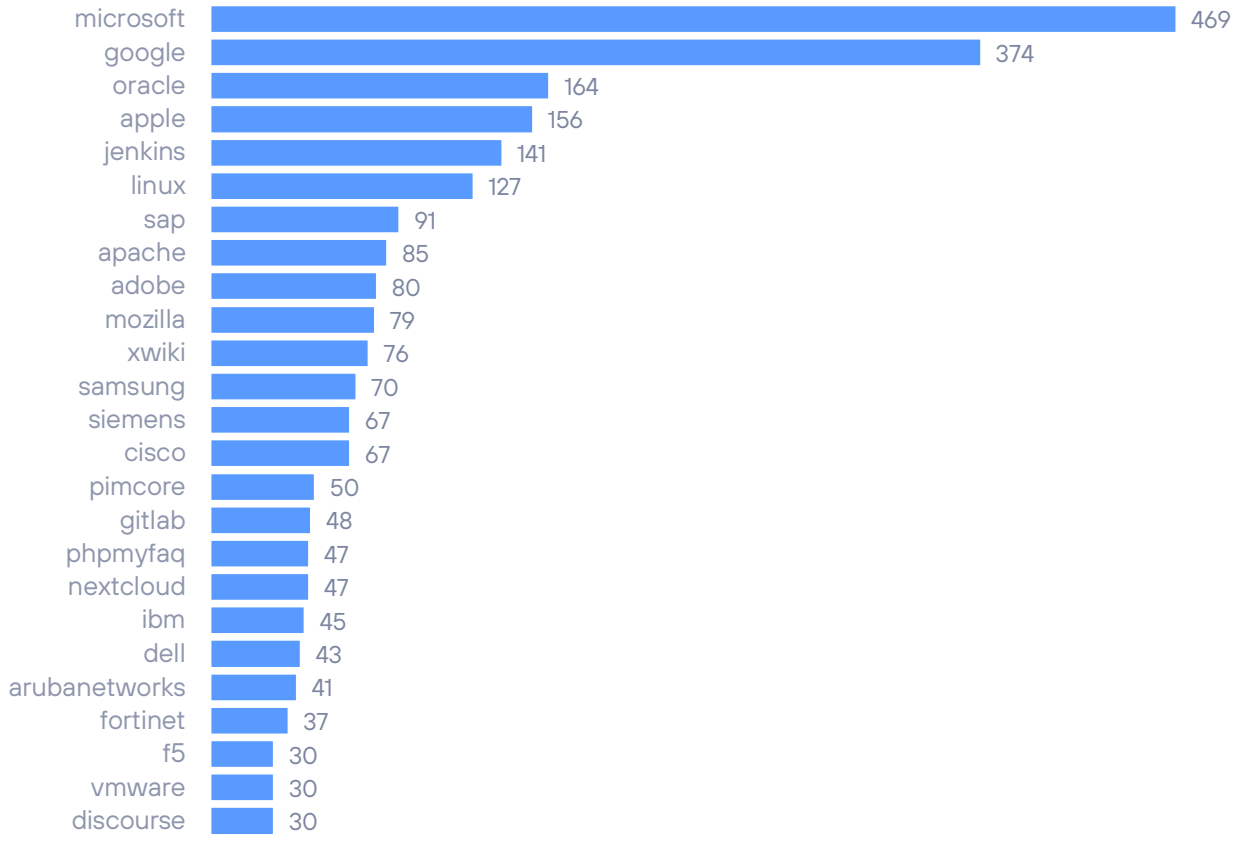


Top 25 compañías con más CVE acumulados

Durante el primer semestre de 2023, Microsoft ha liderado con diferencia por número de vulnerabilidades conocidas, seguido de Google. En general, es habitual que los tres grandes junto con Oracle estén siempre entre los primeros en número de vulnerabilidades.

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 2023

APT 15 - Playful Dragon: un respeto a las canas

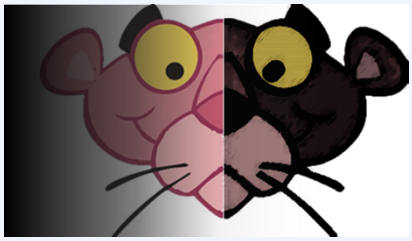
Este grupo de origen chino (AKA "Flea"), catalogado **hace 19 años**, está especializado en ciber-espionaje y fue el creador del RAT "Mirage".

Esta vez, ha sido detectado utilizando la API de "Microsoft Graph" como una backdoor en su última campaña contra ministerios de exteriores de varios países americanos, según indican los investigadores de Symantec.

Además, el grupo utiliza Onedrive como paso intermedio para realizar la conexión con el servidor C&C, que es una técnica que no habían utilizado previamente, aunque se había visto en otro grupo con solera: Swallowtail (AKA APT-28), de origen ruso.

Más información en https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/flea-backdoor-microsoft-graph-apt15

Dark Pink: Pink is the new black



Ya hablamos de este grupo en el informe anterior y siguen siendo tendencia. Descubiertos y catalogados en la segunda mitad de 2022, ahora es más fácil detectar sus movimientos. Se sospecha que lleva desde 2021 ejecutando sus operaciones y enfocado en la zona geográfica de Indonesia (con operaciones en otros países y regiones).

En este semestre, han sido detectados atacando a organizaciones gubernamentales, militares y educativas de su región preferida. Además, han ido renovando y perfeccionando su catálogo de TTP y sus herramientas, lo que indica que están vivos y tienen éxito. Seguro que volvemos a leer sobre ellos...

Más información en: https://www.bleepingcomputer.com/news/security/dark-pink-hackers-continue-to-target-govt-and-military-organizations/

Golden jackal: Demasiado silencioso para ser un chacal...

Este grupo, cuyo nacimiento se estima en 2019, elige como objetivo a entidades gubernamentales y diplomáticas de oriente medio y del sur de Asia. Investigadores de Kaspersky han detallado un interesantísimo artículo donde descubren a un grupo enfocado en el espionaje y con gran capacidad técnica y actitud de sigilo, que son dos características muy poco frecuentes en un chacal.

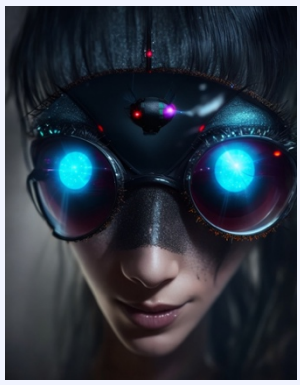
El término "chacal" se utiliza para describir a grupos APT con orientación hacktivista. Los chacales, por lo tanto, suelen ser ruidosos y poco sofisticados. Su actividad, además, se centra en golpes de efecto, por lo que la actividad del espionaje no suele ser su preferida.

Sin embargo, Goldenjackal no es así. Poseen un conjunto de herramientas en .NET propio y bien preparado y sus TTP (las que se conocen) no parecen improvisadas. Leyendo el análisis del equipo de Kaspersky, se percibe que este grupo es minucioso y está muy capacitado. Diríamos, incluso, que parece tener un claro tinte profesional en su manera de prepararlo todo, incluida su versátil catálogo de herramientas. Y, sobre todo, son muy, muy silenciosos. Lista de objetivos muy limitada, poco ruido, cero información publicada...

Respecto a una posible relación con otros grupos, los investigadores observaron similitudes con el grupo APT "Turla" (de supuesto origen ruso) en el algoritmo de generación del UID de la víctima y en las TTP. Sin embargo, las TTP de Goldenjackal no son del todo conocidas y el algoritmo ya era conocido, por lo que tampoco resulta definitivo.

Más información en: https://securelist.com/goldenjackal-apt-group/109677/

Lancefly: La primera mosca que no hace ruido



Ha llegado el verano y hay que hablar de moscas, pero en este caso de "cibermoscas". Este grupo, que actúa en el sur y sureste de Asia, se dedica fundamentalmente a labores de espionaje dirigidas contra entornos gubernamentales, telecomunicaciones y aviación. fue detectado gracias al rastro de una backdoor personalizada que utilizan en sus acciones, Merdoor. Esta puerta trasera fue detectada en 2020, pero el equipo de investigadores de Symantec ha encontrado pruebas de su existencia que se remontan a 2018 y, por lo tanto, fijan también el nacimiento de este APT Group.

Lancefly ha sido incluido en la órbita china debido al uso del mismo RAT que emplea el grupo APT 27 (AKA "Emissary Panda") y a elementos en su rootkit con la misma nomenclatura que los que utiliza también este otro grupo, del que ya os hablamos en el informe anterior. Además, también Lancefly también usa otro RAT, ShadowPad, del que se piensa que es de uso exclusivo de otros "pandas" (APT Groups de origen chino).

Más información en: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor

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.

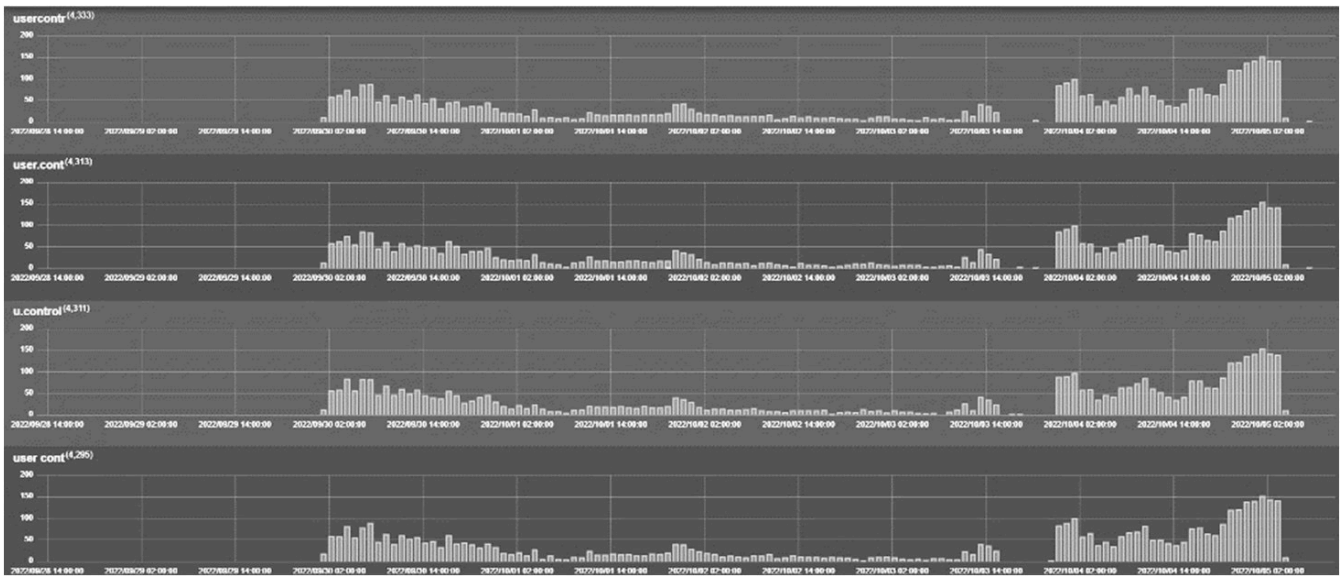
Más información en:
https://aristeo.elevenlabs.tech

Análisis de la información

En el semestre anterior, como caso concreto, analizamos una tabla de intentos de acceso a un sistema de RDP que se encontraba en una bahía de ingeniería (PC de control industrial). Lo que observamos es que los atacantes sabían que ese RDP no era un servicio IT como tal, sino que era una puerta a un sistema de control industrial. Además de intentos de acceso con cadenas que incluían "SCADA" en el top 3, observamos la utilización de nombres propios en los intentos de acceso que, además, iban variando en función de punto de exposición mundial que utilizábamos para el señuelo que expusimos para un cliente del centro de Europa.

Así, cuando expusimos el señuelo en España, los atacantes utilizaban "David", "Laura", "Miguel"... y cuando pasamos por Francia, eran "Isabelle", "Emanuele", "Guillaume"... Cuando situamos el señuelo en una localización diferente, los nombres también variaban y los atacantes utilizaban los nombres más comunes en ese país. Como indicamos en el informe anterior, consultamos los intentos de acceso contra el "INE" (Instituto Nacional de Estadística) de ese país y nos dimos cuenta de que los intentos de acceso utilizaban los 10 nombres más comunes que indicaba este instituto.

Pero esto sólo era un recordatorio ¿Qué más podemos añadir? Además de observar ese dato tan curioso, también demostramos la capacidad de Aristeo de detectar patrones. Vamos a tomar como muestra valores que se repitieron también en España, Francia, y el otro país del que no os podemos comentar nada: "usercontr", "user.cont", "u.control" y "user cont".



Este patrón está tomado recogiendo diferentes direcciones IP y diferentes países **de origen y destino.**

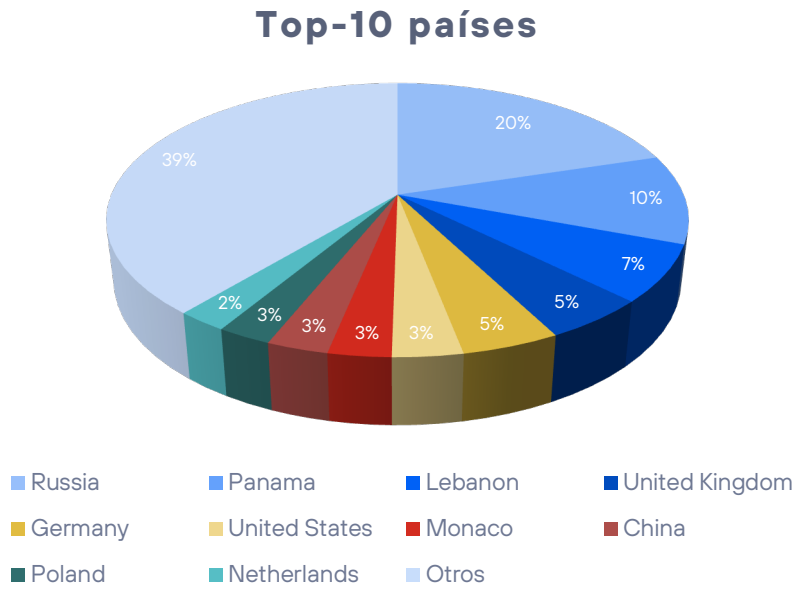
¿Qué quiere decir esto?

Que distintas direcciones IP situadas en distintas partes del mundo estaban ejecutando una misma acción con unas mismas credenciales contra nuestro señuelo industrial. Y, además, este señuelo no estaba situado en un país concreto, sino que lo fuimos "desplazando" por parte de Europa. Por lo tanto, este tipo de intentos constituían **una campaña dirigida contra entornos OT**, al menos dentro del espacio de la UE. Si el objetivo era concretamente el sector industrial, el cliente o todo tipo de entornos OT, eso lo dejamos para nuestro cliente.

Sabemos que estos valores son bastante genéricos, pero nos sirven para que se aprecie rápidamente la similitud entre los valores y el patrón de las detecciones de Aristeo. También detectamos otro tipo de valores relacionados con el cliente y más dirigidos al ámbito OT, pero creemos que esta tupla es un buen botón de muestra.

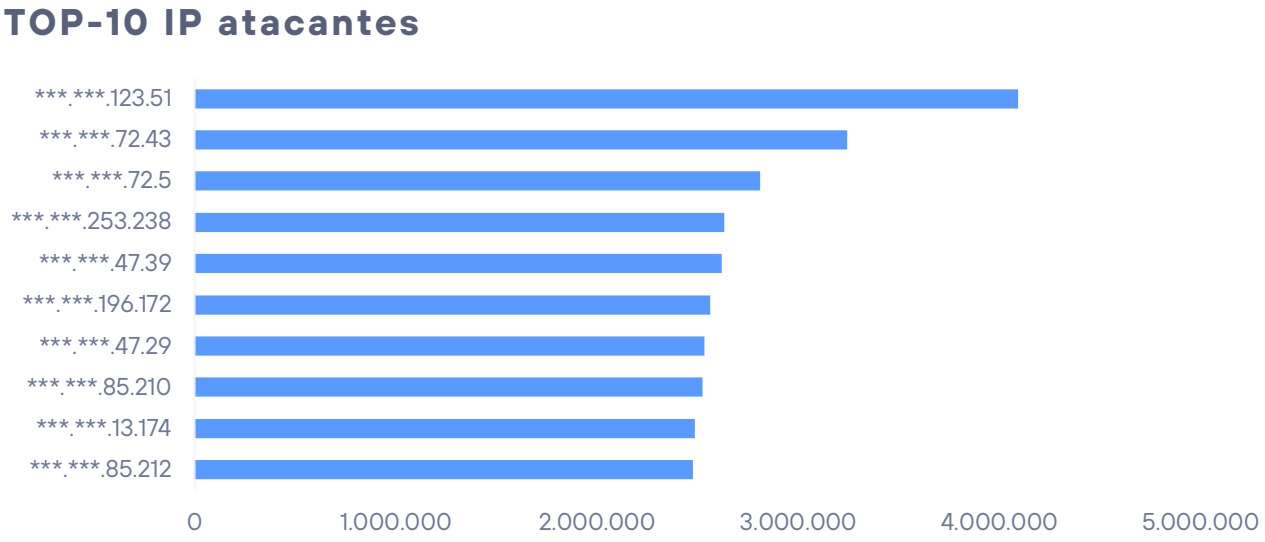
Y ahora, pasamos a la estadística general de la información registrada. En el primer semestre de 2023 se detectaron **más de 300 millones de eventos de ciberseguridad**. Esto supone un ascenso respecto a los datos registrados en el segundo semestre de 2022. Pese a todo, sigue siendo una cifra inferior a los más de 415 millones de eventos detectados en el primer trimestre de 2022.

La distribución por países sería la siguiente:

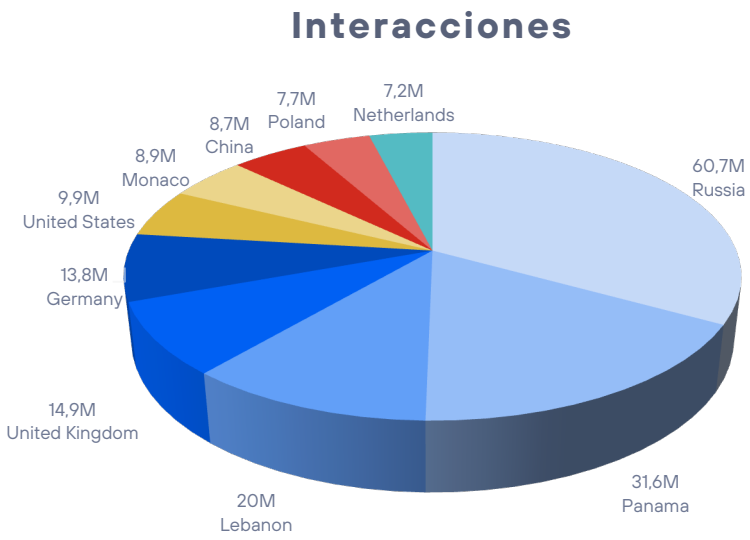


La dispersión geográfica del TOP-10 sigue siendo similar a la de anteriores informes, lo que supone una clara tendencia, pese a que en ocasiones se ve perturbada por sucesos internacionales. También llama la atención el aumento de peso de Panamá, pero de eso hablaremos dentro de dos gráficos.

Ahora vamos a ver las diez direcciones IP con más interacción con el sistema de Aristeo. Algo más del 54% provienen de varios países de Europa del este. En este semestre, el ascenso de Panamá como país de origen también tiene su reflejo en este gráfico. De hecho, casi el 28% de este TOP-10 son direcciones IP con este origen. Sin embargo, hemos detectado que la mayoría de estas direcciones IP tienen salida por Países Bajos. Otras, sin embargo, las capturamos directamente desde Panamá y parece que se trata de sistemas comprometidos.



A continuación, observamos cómo se reparten la actividad los países con más presencia en nuestro Aristeo. En este semestre, el dato llamativo es el ascenso de Panamá como segundo país con más detecciones resulta tan llamativo como el descenso en detecciones de orígenes desde los USA. Desconocemos si estos dos datos están relacionados, y el descenso de resultados desde los USA no podemos analizarlo, pero sí que tenemos la impresión de que los resultados de Panamá se deben a varias campañas contra ciertos objetivos del ámbito financiero en este país.



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: 205.273 direcciones IP, 54892 dominios y 298.086 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 que 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:

Tipo	Cantidad	Porcentaje
Malware Download	150443	50,47%
Phishing	103138	34,60%
Qakbot	18605	6,24%
Malicious URL	11614	3,90%
Cobalt Strike	9397	3,15%
Vidar	1023	0,34%
Raccon	556	0,19%
Astaroth	509	0,17%
Amadey	406	0,14%
DCRat	356	0,12%

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, "Qakbot" cuenta con un número récord dentro de su especialidad: más del 6% del total de URLs están relacionadas con esta familia de malware que hace estragos entre los usuarios de banca online.

¿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.

País	Cantidad	Porcentaje
Estados Unidos	40231	19,60%
China	35111	17,10%
India	14343	6,99%
Rusia	11187	5,45%
Alemania	8775	4,27%
Corea del Sur	5382	2,62%
Singapur	4803	2,34%
Brasil	4429	2,16%
Indonesia	4358	2,12%
Vietnam	3566	1,74%

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?

Tipo	Cantidad	Porcentaje
Mail Spammer	135858	66,18%
Malicious host	57987	28,25%
Proxy	51314	25,00%
SSH Attacker	34879	16,99%
Bruteforce	22928	11,17%
Port scanner	22509	10,97%
Hacking	22199	10,81%
HTTP Spammer	20538	10,01%
HTTP Flooding	19283	9,39%
HTTP Attacker	13087	6,38%

Coronando el ranking 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 es este:

TLD	Cantidad	Porcentaje
com	21219	38,66%
org	2918	5,32%
app	2547	4,64%
top	2522	4,59%
net	1883	3,43%
xyz	1641	2,99%
site	945	1,72%
link	788	1,44%
dev	732	1,33%
click	672	1,22%

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".

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, como se han categorizado estos sobre los últimos seis meses.

Categoría	Cantidad	Porcentaje
Phishing	34697	63,21%
Qakbot	9067	16,52%
Malware download	2048	3,73%
Cobalt Strike	1636	2,98%
Vidar	1527	2,78%
Prometei	1440	2,62%
Astaroth	1031	1,88%
CryptBot	698	1,27%
Infy	648	1,18%
Ice Fog	371	0,68%

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. No obstante, sorprende la cantidad relativa de la familia Qakbot que, al igual que cuando hablamos de URLs, destaca ampliamente sobre el resto de las familias.

Veamos que ocurre en los siguientes seis meses. A ver como fluctúan (o no) las familias de malware en este particular.

RECAPITULACIÓN

Las vulnerabilidades corregidas en iPhone puede que alcancen un buen número este año, atendiendo a las cifras que llevamos en esta primera mitad. En 2022 se alcanzó un récord que no se veía desde 2017. En Android la tendencia es, por el contrario a la baja, con números similares o incluso inferiores este año, cuando la tónica es rondar los 500 fallos. Por el contrario, si 2022 fue uno de los años con menor número de vulnerabilidades críticas, 21, este año ya se ha igualado en solo 6 meses de 2023.

Con respecto al informe de transparencia de Apple, el gobierno alemán vuelve a ser el que más solicitudes ha generado para obtener información sobre dispositivos en el segundo semestre de 2021. Taiwan ha duplicado las solicitudes de información de cuentas por fraude que ha realizado en 2021, pasando de las 1.000 solicitudes de 2020 a las más de 2.000 en 2021. 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 destaca de nuestro análisis es que Brasil está en segundo lugar de una forma muy destacada con 10 veces más solicitudes de preservación y acceso respecto al tercero.

Microsoft, Google y Oracle son las empresas con más fallos corregidos, como de costumbre, aunque a veces intercambiando orden.

Con respecto a la seguridad OT, en el primer semestre de 2023 se detectaron más de 300 millones de eventos de ciberseguridad. Esto supone un ascenso respecto a los datos registrados en el segundo semestre de 2022. Pese a todo, sigue siendo una cifra inferior a los más de 415 millones de eventos detectados en el primer trimestre de 2022.

Del análisis de los datos en Maltiverse, podemos concluir que la mitad de la infraestructura considerada maliciosa se utiliza para descargar malware (un 50%) y que el 66% de las IPs maliciosas se dedican a enviar spam. La infraestructura, en su mayoría, suele estar en EEUU. Aun con la irrupción de nuevos dominios de primer nivel, ".com" sigue siendo el dominio malicioso favorito con un 39% de los casos registrados, muy lejos del segundo ".org" con algo más de un 5%.

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

Web3 y la evolución de la Identidad en Internet

Los ataques más comunes contra las contraseñas y cómo protegerte

INTELIGENCIA ARTIFICIAL Y CRIPTOGRAFÍA

Inteligencia Artificial aplicada a la Ciberseguridad industrial (OT)

Criptografía, una herramienta para proteger los datos compartidos en la red

Edge AI vs. Cloud AI: conoce sus diferencias y elige el mejor enfoque para tu proyecto de Inteligencia Artificial

Evolución de la Ciberseguridad: la IA como herramienta de ataque y defensa

MALWARE

Evolución de las técnicas de Spear-Phishing de los grupos criminales más conocidos y qué malware utilizan

Cibercrimen, una amenaza constante para todo tipo de empresas