Telefónica Tech

Informe sobre el estado de la seguridad 2025 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

INTRODUCCIÓN

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 semestre, destacan dos noticias que, aunque aparentemente no relacionadas, creemos que guardan un denominador común.

En abril de 2025, el gobierno de Estados Unidos anunció que dejaría de financiar a MITRE para operar y mantener el sistema Common Vulnerabilities and Exposures (CVE). Este sistema, está gestionado por MITRE desde 1999 con fondos del Departamento de Seguridad Nacional (DHS) y la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA). Yosry Barsoum, vicepresidente de MITRE, advertía que el contrato expiraría el 16 de abril de 2025 y que, de no renovarse, habría consecuencias graves. La causa principal señalada fue un recorte presupuestario impulsado por la administración Trump, aunque CISA y otras fuentes no detallaron públicamente los motivos exactos. La posible interrupción del servicio generó alarma en la comunidad de ciberseguridad. Por suerte, horas antes del vencimiento, CISA intervino y renovó temporalmente el contrato de MITRE, evitando una interrupción inmediata de los servicios del CVE. Aun así esta solución fue considerada provisional y puso en evidencia la fragilidad de depender de un único financiador gubernamental para un recurso tan crítico.

En respuesta, se anunció la creación de la **CVE Foundation**, una entidad independiente impulsada por miembros del propio consejo del CVE, para garantizar la sostenibilidad y neutralidad del sistema a largo plazo.

Por otro lado, en junio se reveló lo que parecía uno de los mayores incidentes de ciberseguridad de la historia: la filtración de 16.000 millones de contraseñas y credenciales de acceso a servicios como Google, Apple, Facebook, GitHub, Telegram... y hasta portales gubernamentales. La investigación fue liderada por el equipo de Cybernews, que detectó al menos 30 bases de datos de diferentes tamaños, algunas con más de 3.500 millones de registros cada una. No parecía un ataque a una sola empresa, sino una recopilación masiva de robos. Finalmente se supo que el supuesto "leak" de 16.000 millones de contraseñas no era una nueva filtración ni un ataque reciente, sino una compilación de credenciales previamente robadas a lo largo de años mediante malware tipo infostealer, brechas anteriores y ataques de credential stuffing. Los sitios afectados no fueron comprometidos recientemente para obtener estas credenciales.

Lo que ocurrió (como otras veces) es que se recopiló y expuso una base de datos masiva, compuesta por registros ya circulando en foros y mercados clandestinos. No hay evidencia de que contenga datos inéditos (o al menos, no una cantidad relevante) o extraídos de nuevas brechas.

La primera noticia pasó desapercibida para los medios generalistas. Mientras la industria de la ciberseguridad se mordía las uñas durante 24 horas por el miedo a perder el sistema de CVE, el mundo seguía su curso. La segunda noticia, por el contrario, abrió noticiaros genéricos en todos los países, con portadas y reportajes.

Todo el mundo supo del leak. En este caso, el mundo se mordía las uñas mientras la industria sospechaba (por pura lógica) que se trataba de una recopilación de robos antiguos sin mayor trascendencia. Los números no daban tanto de sí en la realidad técnica como en un titular.

Cuando la continuidad del CVE estuvo en peligro, la alarma fue inmediata: expertos, empresas y responsables de seguridad comprendieron que perder esta infraestructura suponía volar a ciegas ante las vulnerabilidades, un caos que afectaría a la respuesta a incidentes, la protección de infraestructuras y la coordinación global. Sin embargo, el "leak" de contraseñas, a pesar de su enorme eco mediático, no generó la misma preocupación profesional porque, en el fondo, no alteraba el panorama de amenazas ni introducía riesgos nuevos: era, sobre todo, ruido y reciclaje de datos ya expuestos.

Este fenómeno pone de manifiesto una brecha persistente entre lo que realmente importa en la industria para la resiliencia digital y lo que capturan los titulares. Los medios tienden a amplificar los incidentes más espectaculares o fáciles de entender, aunque su impacto real sea limitado, mientras que los problemas estructurales —como la financiación y gobernanza de infraestructuras críticas— quedan relegados o pasan desapercibidos.

Esto no solo distorsiona la percepción del usuario, que a menudo termina creyendo cualquier alarma amplificada sin contexto, sino que también refleja una cierta inmadurez en la cobertura informativa: rara vez se consulta a los expertos adecuados ni se explican las consecuencias técnicas de fondo. La industria, por su parte, demuestra que lo realmente importante no siempre es lo más visible, y que la seguridad depende más de la solidez de sus cimientos —como el CVE— que de la espectacularidad de los incidentes que copan portadas. ¿Estamos todavía quizás, muy alejados del usuario?

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 2025

A continuación, damos cuenta de aquellas noticias que mayor impacto han tenido durante el transcurso de este primer semestre de 2025.

ENERO

- Se identifica un fallo que permite recuperar imágenes de hibernación en texto claro, exponiendo potencialmente contraseñas y datos sensibles si un atacante tiene acceso físico al disco duro cifrado con BitLocker (CVE-2025-21210). No fue el único problema con esta tecnología este año.
- **Se descubren dos graves vulnerabilidades en SAP: CVE-2025-0070,** Autenticación incorrecta en SAP NetWeaver AS para ABAP y ABAP Platform, que permitía a un atacante autenticado obtener acceso ilegítimo al sistema explotando comprobaciones de autenticación inadecuadas. Además de CVE-2025-0066, una divulgación de información en SAP NetWeaver AS para ABAP y ABAP Platform (Internet Communication Framework).
- Un grupo de llamado **"Belsen Group"** filtró gratuitamente en la dark web los archivos de configuración, direcciones IP y credenciales VPN de más de 15.000 dispositivos FortiGate de todo el mundo, tanto del sector público como privado. El volcado, de 1,6 GB, incluye información sensible como contraseñas en texto claro, claves privadas y reglas de firewall, y fue recolectado tras explotar la vulnerabilidad CVE-2022-40684 en 2022.
- **Moxa,** proveedor de comunicaciones y redes industriales, **publicó el día 3 de enero un aviso urgente sobre dos vulneraciones de alto impacto.** Además, para algunos dispositivos afectados no existía en ese momento otra cosa que no fueran medidas de mitigación. Una de estas vulnerabilidades permitía tomar el control de los dispositivos y sistemas afectados remotamente.
- Xlab publicó una investigación sobre una botnet basada en Mirai que está explotando vulnerabilidades 0-day en routers industriales y del hogar. La botnet maneja unos 15.000 bots diariamente y la mayoría se encuentran en USA, China, Rusia, Irán y Turquía. La actividad más común de esta botnet son los ataques DDoS.
- Aunque ocurrió en octubre, se dio a conocer en enero. **Cloudflare mitigó el mayor ataque DDoS registrado hasta la fecha,** que alcanzó un pico de 5,6 terabits por segundo. El ataque, lanzado por una botnet basada en Mirai con 13.000 dispositivos comprometidos, tuvo como objetivo un proveedor de servicios de Internet en Asia Oriental y duró solo 80 segundos.

FEBRERO

- **En septiembre de 2024 se detectó una vulnerabilidad zero-day en 7-Zip** (CVE-2025-0411) que permitía a atacantes rusos eludir la protección de "Mark of the Web" (MoTW) en Windows mediante archivos comprimidos doblemente anidados. Este fallo fue explotado durante febrero en campañas de phishing dirigidas a organismos gubernamentales y empresas ucranianas, permitiendo la ejecución de malware como SmokeLoader sin mostrar advertencias de seguridad al usuario.
- **Al menos 28 aplicaciones en Google Play y la App Store de Apple incluían un software malicioso,** conocido como SparkCat o SparkKitty, diseñado para robar frases de recuperación de monederos de criptomonedas mediante técnicas de reconocimiento óptico de caracteres (OCR).

Este malware, oculto en apps legítimas y descargado más de 242.000 veces, accedía a la galería de imágenes del dispositivo y buscaba capturas de pantalla con palabras clave asociadas a criptomonedas, permitiendo a los atacantes vaciar los fondos de las víctimas. **Es la primera vez que un stealer de este tipo logra infiltrarse en la App Store,**

- El FBI responsabilizó a Corea del norte, a través del APT Group "Lazarus", del **robo de 1.500 millones de dólares al Exchange de criptoactivos Bybit.** En esta operación, que el FBI llamó "TraderTraitor" y está catalogada como el mayor robo de criptoactivos de la historia, los delincuentes lograron vulnerar una de las carteras frías, consideradas seguras, accediendo a los fondos y dividiéndolos en múltiples billeteras para dificultar su rastreo
- **Lee Enterprises,** uno de los grupos de periódicos más grandes de Estados Unidos**, dice que un ciberataque que afectó sus sistemas** causó una interrupción en febrero e impactó sus operaciones. Esas operaciones incluyeron acceso de los trabajadores al sistema, por lo que no fue posible entregar artículos, imprimir y entregar docenas de periódicos.
  Esta empresa, que publica 77 diarios con una tirada diaria de 1,2 millones de ejemplares, 350 semanarios y ediciones digitales con más de 44 millones de visitantes únicos, ya fue atacada en 2020 por ciberdelincuentes iraníes durante la campaña electoral presidencial.
- **Según chainAnalysis, en 2024, los pagos por ransomware cayeron un 35%** respecto al año anterior, totalizando 813,55 millones de dólares frente a los 1.250 millones de 2023, a pesar de que el volumen de ataques alcanzó cifras récord. Solo el 30% de las víctimas que negociaron con ciberdelincuentes acabaron pagando.
- **Se descubrieron dos vulnerabilidades críticas en OpenSSH:** una, identificada como **CVE-2025-26465,** permitía ataques de tipo (MitM) contra clientes OpenSSH cuando la opción VerifyHostKeyDNS estaba activada. Este fallo existía desde 2014 y afectó especialmente a sistemas FreeBSD donde la opción estaba habilitada por defecto. La segunda, **CVE-2025-26466**, introducida en 2023, permitía ataques de denegación de servicio (DoS) antes de la autenticación.

MARZO

- El grupo de investigación **GreyNoise, detectó una campaña de backdoor que afecta a miles de enrutadores ASUS.** Según los investigadores, este movimiento estaría enfocado al establecimiento de una futura botnet.
- Investigadores de Proofpoint identificaron una campaña por correo electrónico muy dirigida a menos de cinco clientes de Proofpoint en los Emiratos Árabes Unidos relacionados con aviación y comunicaciones satelitales, además de infraestructura de transporte crítica. En esta campaña se descubrió una backdoor denominada Sosano y la utilización de ficheros polyglots para ofuscar el contenido del payload. Estos ficheros están especialmente diseñados para que distintas aplicaciones los interpreten como tipos de fichero distinto.
- **Investigadores de Truffle Security descubrieron casi 12.000 claves API** y contraseñas válidas (incluyendo credenciales de AWS, MailChimp y WalkScore) dentro del conjunto de datos Common Crawl, ampliamente utilizado para entrenar modelos de inteligencia artificial de empresas como OpenAI, Google y Meta, muchas de ellas hardcodeadas en HTML y JavaScript.
- **YouTube alertó sobre una sofisticada campaña de phishing** en la que ciberdelincuentes emplean un vídeo generado por inteligencia artificial que simula al CEO de la plataforma, Neal

Mohan, anunciando falsos cambios en la política de monetización. Los atacantes envían este deepfake como video privado a creadores de contenido, junto con correos que incluyen enlaces a una página falsa de verificación del Programa de Socios de YouTube. Al intentar "confirmar" los nuevos términos, las víctimas entregan sus credenciales.

- Investigadores identificaron una **campaña masiva de malware denominada "Vapor", en la que 331 aplicaciones maliciosas en Google Play**, disfrazadas de utilidades como rastreadores de salud, optimizadores de batería o escáneres QR, lograron más de 60 millones de descargas. Estas apps, inicialmente legítimas para superar los controles de Google, descargaban código malicioso tras su instalación para mostrar anuncios intrusivos, robar credenciales y datos de tarjetas mediante phishing, y dificultar su eliminación ocultando su icono y actividad.
- Investigadores alertaron sobre la **explotación masiva de la vulnerabilidad crítica CVE-2024-4577 en PHP para Windows,** que permite la ejecución remota de código en servidores que utilizan PHP en modo CGI. Aunque el fallo fue parcheado en junio de 2024, atacantes aprovecharon rápidamente el exploit, especialmente en Japón, y luego a nivel global, con más de 1.000 IPs únicas intentando explotar la vulnerabilidad solo en enero.

ABRIL

- El FBI, a través del Centro de Quejas y Delitos en Internet (IC3), afirmó que **EE.UU. perdió en 2024 más de 16.600 millones de dólares.** Como referencia, en 2023 las pérdidas reportadas fueron de 12.500 millones de dólares. Debe advertirse que, aunque la cifra sea muy llamativa, sólo refleja la actividad detectada por el IC3 o denunciada por las víctimas, por lo que supone sólo una parte del monto final.
- La empresa de diálisis renal **DaVita reveló que sufrió un ataque de ransomware que cifró partes de su red e impactó algunas de sus operaciones.** Días más tarde, el grupo de ciberdelincuentes Interlock se atribuyó el ataque y anunció que tenía 20 terabytes de información confidencial de la compañía. Según este mismo grupo, las negociaciones con la empresa no fructificaron, por lo que pusieron la información a la venta.
  DaVita tiene unos ingresos anuales que superan los 12.800 millones de dólares.
- **GitHub detectó más de 39 millones de secretos filtrados en repositorios,** incluyendo claves API y credenciales, lo que expuso a usuarios y organizaciones a graves riesgos de seguridad. A pesar de medidas como la protección de push activada por defecto en repositorios públicos.
- Se descubrió una **vulnerabilidad crítica de ejecución remota de código (RCE) en Apache Parquet,** un formato de almacenamiento de datos ampliamente usado en entornos de big data y análisis, especialmente en plataformas como Hadoop, AWS, Google Cloud y Azure. Identificada como CVE-2025-30065 y con una puntuación máxima CVSS 10.0.
- En abril se descubrió una campaña masiva en la que al menos **diez extensiones maliciosas para Visual Studio Code, publicadas en el marketplace oficial de Microsoft, infectaron a miles de usuarios de Windows con el cryptominer XMRig** para Monero. Estas extensiones, que simulaban ser herramientas legítimas de desarrollo como "Prettier", "Discord Rich Presence" o "Solidity Compiler", acumulaban cientos de miles de descargas, muchas de ellas infladas artificialmente para aparentar popularidad.

- **Google Chrome 136 solucionó una vulnerabilidad que llevaba más de 20 años permitiendo a los sitios web identificar el historial de navegación de los usuarios** mediante el análisis del color de los enlaces visitados con el selector CSS :visited. Este fallo permitía a páginas maliciosas rastrear, perfilar e incluso lanzar ataques de phishing al detectar qué enlaces había visitado un usuario en otros sitios.

MAYO

- **Una operación policial conjunta** llevada a cabo por autoridades holandesas y estadounidenses **desmanteló una botnet formada por unos 7.000 dispositivos de Internet de las cosas (IoT) y otros en estado de final de vida útil (EoL - End of life).** La red se alquilaba para proporcionar anonimato a los atacantes. Éstos pagaban entre 9.95 y 110 dólares al mes, lo que generó unos ingresos de más de 46 millones de dólares.
- **Arla Foods, gigante danés** de la industria alimentaria, **confirmó que había sido objeto de un ciberataque que interrumpió sus operaciones** de producción en una planta lechera de Alemania. Este ataque forzó a la compañía a informar a sus clientes de retrasos en sus pedidos.
- **Se detectó un ataque a la cadena de suministro dirigido a servidores Linux,** donde tres módulos maliciosos de Go publicados en GitHub contenían código ofuscado que descargaba y ejecutaba un script Bash capaz de sobrescribir por completo el disco principal (/dev/sda) con ceros. Esta acción provocaba la pérdida total e irreversible de datos y dejaba los sistemas inservibles. Los módulos, que imitaban proyectos legítimos, fueron retirados rápidamente.
- **La organización criminal LockBit sufrió una brecha interna cuando sus paneles de administración y afiliados en la dark web fueron atacados y reemplazados por un mensaje de advertencia** junto a un enlace para descargar una copia de su base de datos MySQL. El volcado expuso detalles operativos clave: más de 59.000 direcciones de bitcoin, configuraciones de ataques, credenciales de afiliados y, especialmente, más de 4.400 registros de negociaciones entre víctimas y extorsionadores desde diciembre de 2024.
- **Investigadores descubrieron una campaña masiva que introdujo más de 100 extensiones maliciosas en la Chrome Web Store,** haciéndose pasar por herramientas legítimas como VPNs, asistentes de IA y utilidades de marcas reconocidas como Fortinet y YouTube. Estas extensiones, promocionadas a través de sitios web falsos y malvertising, ofrecían parte de la funcionalidad prometida, pero en realidad robaban cookies, credenciales y datos de navegación, podían ejecutar scripts remotos, modificar el tráfico y convertir el navegador en un proxy para los atacantes.

JUNIO

- **WestJet, la segunda aerolínea más grande de Canadá, confirmó un ciberataque que interrumpió el acceso a algunos sistemas internos.** El ataque también impidió que los usuarios iniciaran sesión en el sitio web y en la aplicación móvil, servicios que ahora están restablecidos.
- Un nuevo ataque denominado **'SmartAttack' utiliza relojes inteligentes como receptores de señales ultrasónicas encubiertos para extraer datos** de sistemas aislados físicamente a través de la técnica “Airgap”, utilizada en muchos entornos industriales. Además, esta técnica puede interferir en el rendimiento de la RAM, las pantallas, cables SATA... etc. Aunque la recepción de esas

señales pueda hacerse a través del Smartwatch, aun así alguien debe haber comprometido el dispositivo aislado por Airgap.

- **En junio de 2025 se reveló CVE-2025-49113, una vulnerabilidad crítica de ejecución remota de código (RCE) en Roundcube Webmail** que afecta a todas las versiones desde la 1.1.0 hasta la 1.6.10. El fallo, causado por la falta de validación en el parámetro _from en el script upload.php, permite a un atacante autenticado ejecutar código malicioso en el servidor, comprometiendo la seguridad de la plataforma. Más de 84.000 instancias de Roundcube permanecen vulnerables.
- Se reportó que **más de 46.000 instancias de Grafana expuestas a Internet siguen vulnerables** al fallo crítico CVE-2025-4123, un problema de redirección abierta y XSS que permite a atacantes ejecutar plugins maliciosos y secuestrar cuentas de usuario mediante un simple enlace. El exploit, que no requiere privilegios elevados y puede funcionar incluso con acceso anónimo habilitado, permite el robo de sesiones, el cambio de credenciales y, en algunos casos, ataques SSRF contra sistemas internos.
- **En junio de 2025 se descubrieron dos vulnerabilidades críticas de escalada local de privilegios en Linux, CVE-2025-6018 y CVE-2025-6019,** que permiten a cualquier usuario con acceso a una sesión (incluso por SSH) obtener permisos de root en la mayoría de las distribuciones modernas. El primer fallo, en la configuración de PAM de SUSE, otorga privilegios de “allow_active” a usuarios remotos; el segundo, en libblockdev y el demonio udisks (presente por defecto en casi todos los sistemas Linux), permite a estos usuarios elevarse a root con muy poco esfuerzo.

MÓVILES

Apple iOS

Las mejoras de seguridad de iOS 18

Tendremos que esperar hasta después del verano para conocer las mejoras en seguridad de la nueva versión de iOS.

Hasta ahora, lo que sí sabemos es que no se llamará iOS 19 sino iOS 26. Se pasa de una numeración lineal a nombrar los sistemas operativos de manera unificada según el año; aunque a pesar de que se publique en 2025 se adelantará la denominación al siguiente.

En el siguiente informe desgranaremos las novedades en materia de seguridad que nos traerá iOS 26.

Vulnerabilidades y versiones publicadas en el primer semestre de 2025

Cerramos 2024 con iOS 18.2. El 2025 no tuvo que esperar mucho para ver una actualización, aunque en este caso no portaba ninguna corrección de seguridad. El 6 de enero se publica la 18.2.1.

No fue hasta el 27 de enero cuando llegan los primeros parches. Es ese día cuando se publica iOS 18.3 con 38 CVEs, algunas de ellas afectando al kernel y que podrían ejecutar código arbitrario o elevar privilegios. Anotar, que el CVE-2025-24085, un fallo en CoreMedia estaba siendo explotado activamente por atacantes para elevar privilegios en versiones de iOS anteriores a 17.2.

El 10 de febrero amanecía con una actualización de urgencia, iOS 18.3.1: un parche que corregía una vulnerabilidad muy particular, dado que se tenía constancia de que había sido aprovechada en un

ataque específico contra un objetivo de interés. En concreto, el parche corrige el acceso a un iPhone bloqueado (CVE-2025-24200).

No terminan los sustos ahí. Precisamente, el 11 de marzo se publica 18.3.2 con otro fallo que había sido usado en ataques quirúrgicos, contra objetivos muy precisos. En esta ocasión se trataba de una escritura fuera de límites de un búfer de WebKit (componente web) y se le asignó el CVE-2025-24201.

De hecho, con la gravedad que suponen las dos vulnerabilidades comentadas, Apple decide publicar una actualización para terminales más antiguos, el 31 de marzo se liberan, 15.8.4 y 16.7.11 respectivamente, para cubrir dispositivos más antiguos.

Ese mismo día, se publica 18.4 con nada más y menos que 75 vulnerabilidades únicas parcheadas. A pesar del número, solo una de ellas permite ejecutar código arbitrario (CVE-2025-24243) a través del componente de Audio.

El 16 de abril aparecen dos nuevos parches críticos con 18.4.1. Se corrigen fallos que estaban siendo explotados en operaciones contra perfiles muy concretos; mismo caso que los ya comentados con anterioridad. Uno en el componente CoreAudio y otro en RPAC (Reconfigurable Preprocessing Architecture Core)

Hasta el 12 de mayo, fecha en la que se publica iOS 18.5, no hay más sobresaltos. En este grupo de parches encontramos hasta 33 vulnerabilidades corregidas, dos de ellas permitían la ejecución de código arbitrario.

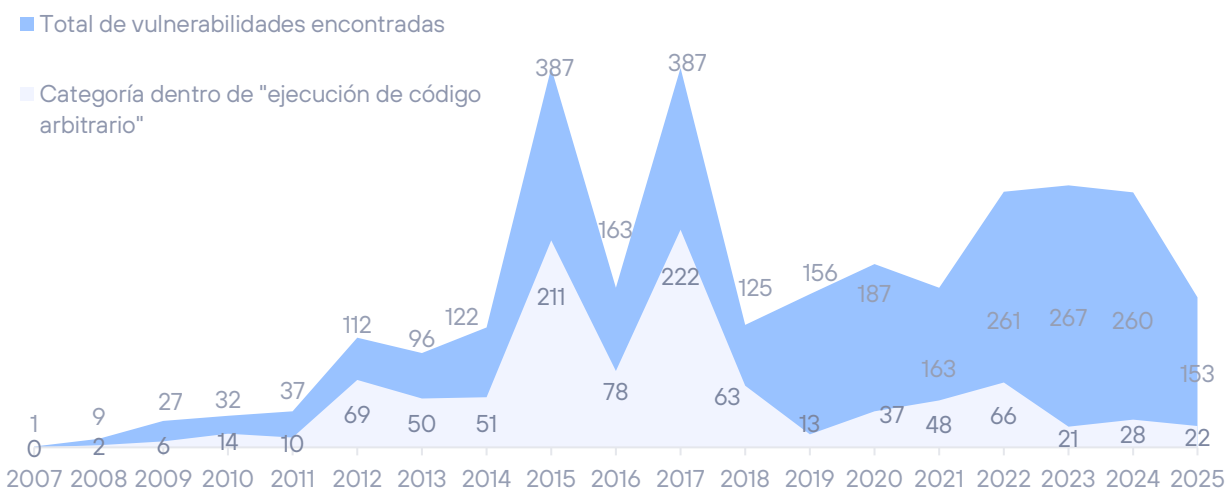
Evolución de vulnerabilidades en iOS durante el primer semestre de 2025

El Segundo semester de 2024 se cerró con 149 vulnerabilidades parcheadas, cuatro consideradas de alto reiesgo, con posibilidad de ejectutar código arbitrario.

Un número similar al del primer semester de 2025, que lo supera ligeramente con 153 parches.

VULNERABILIDADES EN IOS 2025-H1

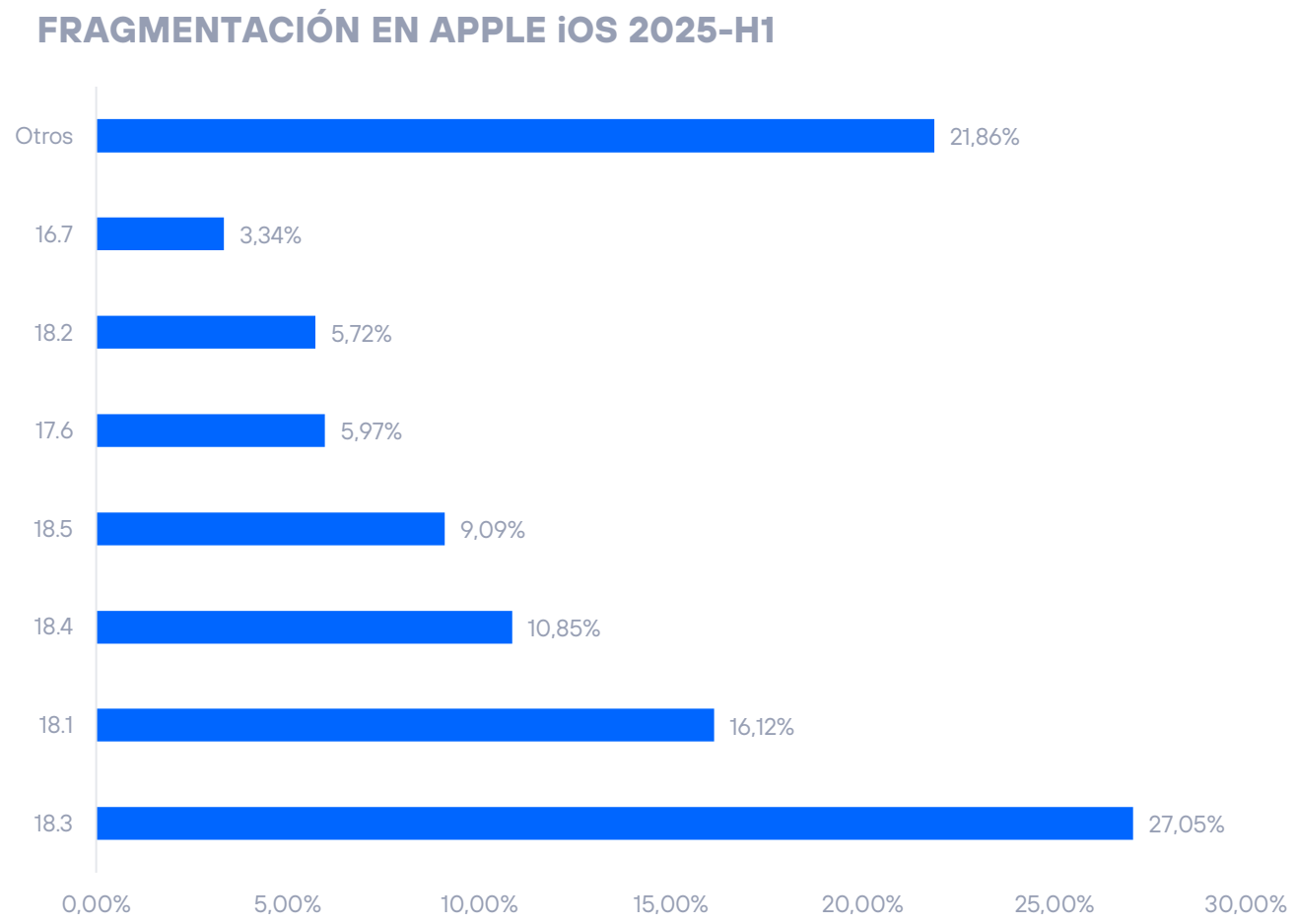
Evolución de vulnerabilidades por año



Fragmentación de versiones durante el primer semestre de 2025

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.

Y no es para menos. Los cuatro primeros puestos del share son ocupados por iOS 18 y sus diferentes versiones



Eso sí, tenemos un 21.86% de cuota que no especifica versión, con lo cual es un saco de versiones que no podemos identificar y podrían estar soportadas o no.

La última versión con soporte de Apple es la iOS 15, estrenada en septiembre de 2021.

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 2023 y primer semestre de 2024 (el último publicado por Apple a fecha del primer semestre de 2025)** 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.

País	Peticiones 2023-H2	Aceptadas 2023-H2	Peticiones 2024-H1	Aceptadas 2024-H1	Suma	% Aceptadas
Estados Unidos	6.410	5.233	12.043	10.377	18.543	85%
Alemania	8.866	4.463	9.778	4.713	18.644	49%
China	905	853	1.212	1.146	2.117	94%
Brasil	5.858	4.765	8.776	6.808	14.634	79%
Reino Unido	1.633	1.337	2.925	2.278	4.558	79%
España	620	290	540	186	1.160	41%

Como viene siendo habitual, Alemania lidera las solicitudes de información sobre dispositivos, si bien en 2024 Estados Unidos repuntaba con fuerza. Brasil también es un actor destacado en este punto. En España se observa un detalle curioso: la tasa de aceptación es bastante baja.

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.

País	Requests 2023-H2	Data Prov. 2023-H2	Requests 2024-H1	Data Prov. 2024-H1	Suma	% Aceptadas
Taiwan	4.415	4.345	4.968	4.819	9.383	98%
Japón	477	300	1.345	1.142	1.822	79%
China	327	278	465	361	792	81%
Estados Unidos	1.018	744	1.341	930	2.359	71%
Corea del Sur	154	131	199	111	353	69%
España	593	197	640	224	1.233	34%

De nuevo Taiwán sobrepasa a Estados Unidos en las solicitudes de información por fraude durante el segundo semestre de 2023 y primero de 2024. España ocupa una posición destacada, igualmente, como el caso anterior, con muy baja tasa de aceptación.

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...).

País	Requests 2023-H2	Requests 2024-H1	Suma	% Aceptadas 23H2	% Aceptadas 24H1
Estados Unidos	10.827	12.812	23.639	90%	90%
Alemania	1.925	2.655	4.580	63%	65%
Brasil	3.327	3.664	6.991	62%	71%
Reino Unido	1.414	2.550	3.964	81%	82%
Japón	259	841	1.100	55%	77%
España	101	156	257	34%	36%

Estados Unidos vuelve a liderar holgadamente las solicitudes de información de cuentas enviadas a Apple durante el final de 2023 y principios de 2024.

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.

País	Requests 2023-H2	Preserved 2023-H2	Requests 2024-H1	Preserved 2024-H1
Estados Unidos	6.610	16.682	8.170	20.513
Brasil	242	466	264	407
Reino Unido	47	54	64	99
Alemania	53	61	52	50
Francia	2	6	41	85
España	1	1	0	0

Estados Unidos, de lejos, el país con más peticiones, seguido de Brasil. En este aspecto, España apenas realiza este tipo peticiones.

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.

País	Requests 2023-H2	Data Prov. 2023-H2	Requests 2024-H1	Data Prov. 2024-H1	Suma Data Prov.
Reino Unido	655	597	726	658	**1.255**
Estados Unidos	636	451	793	601	**1.052**
Japón	259	215	288	239	**454**
Canadá	147	125	169	141	**266**
Alermania	99	73	99	74	**147**
España	5	3	1	1	**4**

El Reino Unido sigue siendo el que más demanda estas peticiones a Apple, con buena parte satisfechas.

Peticiones relacionadas con la retirada de apps del market

Este dato ya no se ofrece en el informe de Apple. Actualizaremos el siguiente con más información y las novedades en el informe de transparencia de Apple.

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

Estrenamos Android 16

El 10 de junio de este año, Android estrenaba la versión 16 del sistema operativo de Google. Veamos qué novedades respecto al capítulo de seguridad nos trae.

Advance Protection 2

En mayo de 2025, Google anunció una característica de seguridad llamada Advanced Protection para dispositivos Android. Esta función está dirigida a usuarios con un perfil de riesgo elevado, como periodistas, activistas o figuras públicas u otros perfiles de interés, pero puede ser activada por cualquier persona que desee reforzar la seguridad de su dispositivo móvil. En cierta forma, es similar a la funcionalidad de "Security LockDown" disponible en iOS desde hace algunos años.

Advanced Protection reúne múltiples medidas de protección que ya existían en Android, pero las agrupa bajo un único sistema que puede activarse de forma sencilla a partir de Android 16. Al activarlo, se bloquean varias configuraciones del sistema para impedir su desactivación accidental o intencionada por parte del malware o de terceros con acceso físico al dispositivo. Esta activación también ajusta automáticamente ciertos parámetros de seguridad en aplicaciones de Google, como Chrome, Mensajes o Teléfono, entre otras.

Entre las funciones que incluye se encuentra un sistema de análisis local más riguroso de aplicaciones mediante Google Play Protect, que mejora la detección de software potencialmente dañino. También se ha anunciado una futura característica denominada “Intrusion Logging”, que registrará eventos relevantes del sistema para facilitar el análisis forense en caso de compromiso. Este registro se almacena en una ubicación protegida, inaccesible incluso para usuarios con privilegios elevados.

Además, el programa contempla mejoras en la protección frente a conexiones físicas o de red potencialmente peligrosas. En futuras actualizaciones, se espera que Advanced Protection bloquee automáticamente conexiones por USB con dispositivos no autorizados, así como desconecte el teléfono de redes Wi-Fi abiertas que se consideren de riesgo. También se integrará con funciones del sistema para detectar posibles estafas telefónicas.

Advanced Protection está diseñado para evolucionar con el tiempo, añadiendo nuevas capas de seguridad sin necesidad de intervención por parte del usuario. Su activación no requiere conocimientos técnicos avanzados, y busca equilibrar la facilidad de uso con un nivel de protección superior al estándar que ofrece Android por defecto.

Prevención de fraudes durante las llamadas

Interesante medida adoptada en Android. Durante las llamadas se impedirá la desactivación de Google Play Protect para impedir que mediante ingeniería social se convenza al usuario de la instalación de una aplicación maliciosa. Además, se está explorando el uso de la IA para verificar si una llamada es fraudulenta.

Wifi

Android 16 permite conectarse a redes WiFi 6 o 802.11az que poseen cifrado AES-256 y protección contra ataques de hombre-en-el-medio.

Registro de eventos de seguridad

Otra medida interesante. Un registro de eventos de seguridad que es almacenado en una zona del dispositivo de difícil acceso incluso para usuarios con privilegios avanzados.

Esto facilita obtener un registro de eventos en dispositivos que hayan sido objeto de ataques o infecciones. La idea es que no sea accesible con facilidad pero que sirva para que equipos forenses puedan extraer dichos eventos cuando se realiza un análisis del dispositivo. Una especie de "caja negra" virtual.

Vulnerabilidades

Android publica un conjunto de parches cada mes, generalmente durante la primera semana.

En este primer semestre de 2025 se han publicado seis boletines con la siguiente distribución de vulnerabilidades por cada mes:

Mes	CVEs	Críticos o RCE
Enero	34	6
Febrero	46	1
Marzo	41	10
Abril	57	4
Mayo	46	1
Junio	34	0

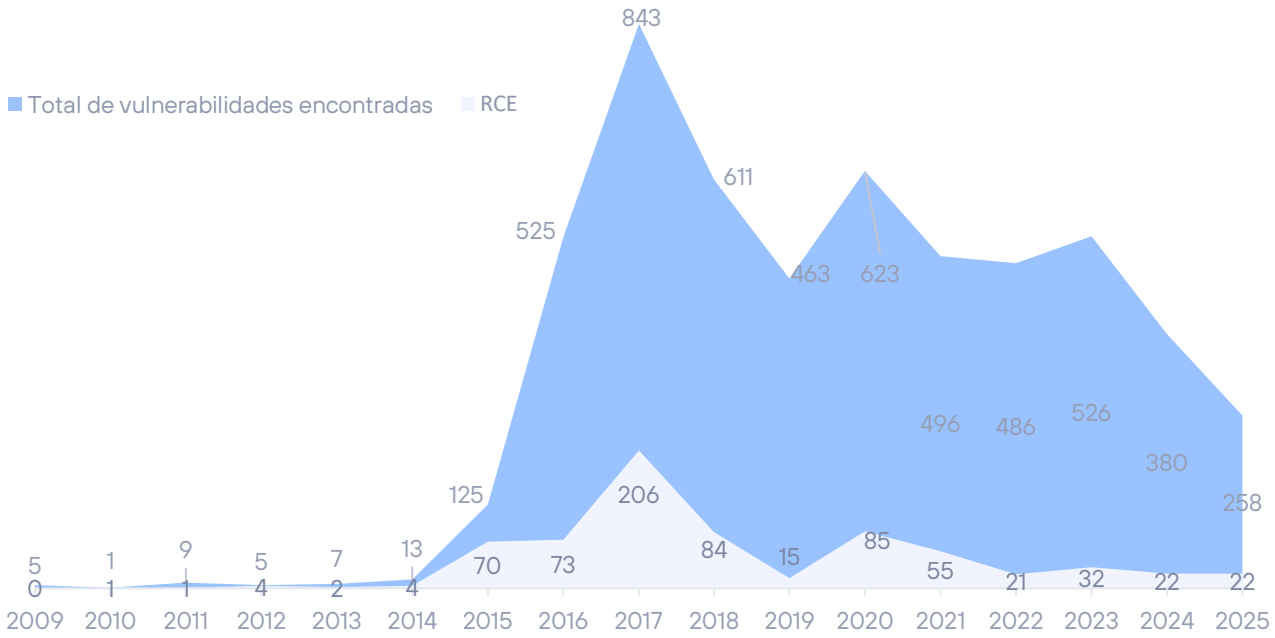
No obstante, algunos CVE pueden no poseer información de su impacto asociado a fecha de publicación de este informe, por lo que posteriormente el número de estos puede ser superior al indicado.

En total, 258 parches en este semestre (el semestre anterior fue de 167); 22 de ellos considerados críticos (10 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 2025-H1

Evolución de vulnerabilidades por año



Fragmentación en sistemas Android

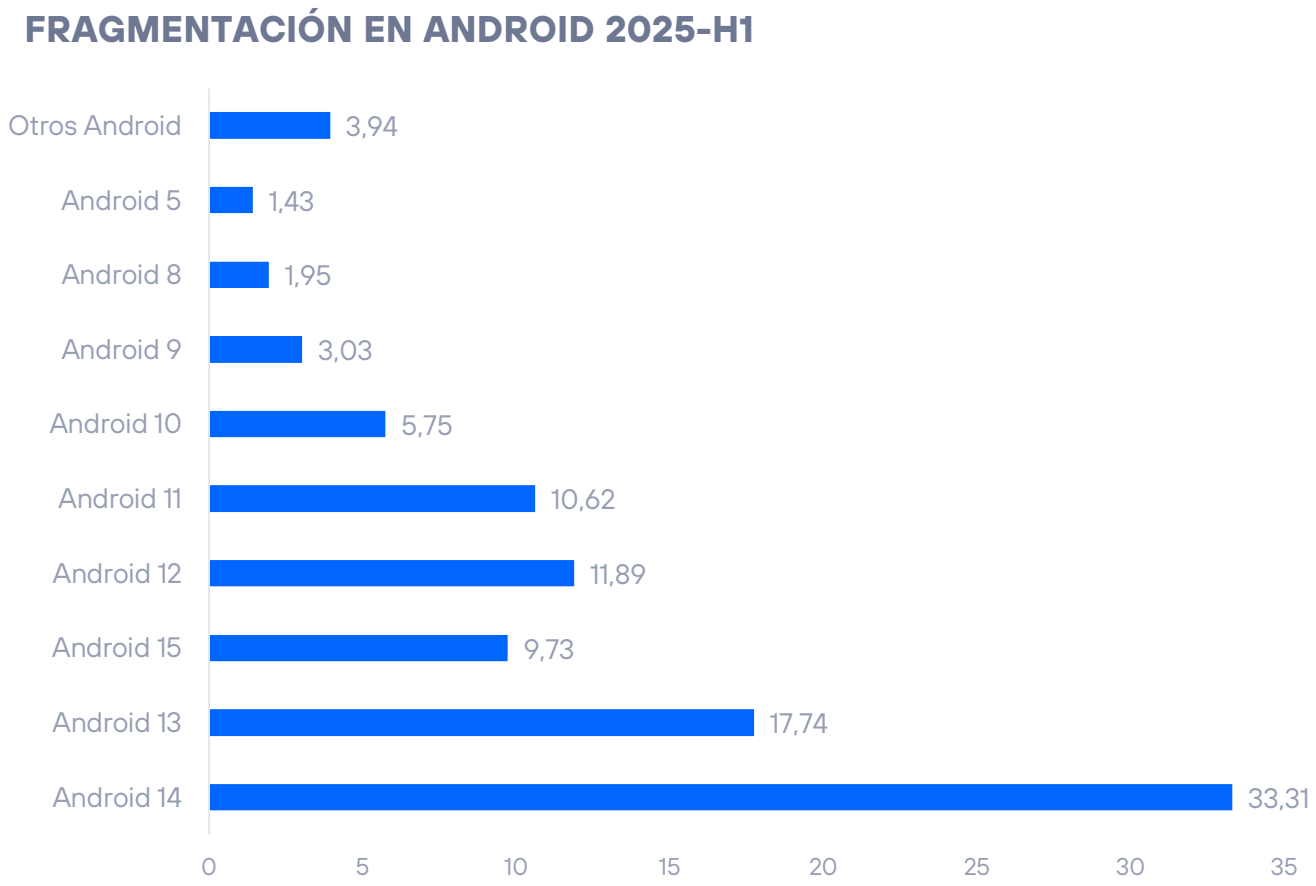
La última publicación de Statcounter a fecha de edición de este informe nos indican que la versión más implantada de Android sigue siendo la 14, con un share de 33.31% que incluso supera al 25.64% del semestre pasado. Es decir, a pesar de la salida de Android 15 en octubre del 2024, 14 sigue creciendo en su base de usuarios.

Android 15 aún no ha tenido un efecto notable en el parque de dispositivos móviles de dicho sistema. Habrá que esperar a la nueva edición de este informe para evaluar la situación. Es notable incluso el aumento en cifras de la versión anterior, la 14, que ha crecido incluso en penetración; algo que ya dijimos y ocurría en el informe anterior. De hecho, nos sorprende que el crecimiento de 14 es incluso más agudo que el semestre pasado. Habrá que esperar un semestre más para ver la evolución de share de la versión 15.

Las versiones de Android anteriores a la versión 13 (versión publicada en agosto de 2022) ya no tienen soporte de actualizaciones.

El ranking sigue habituándonos a ver un share preocupante de versiones de Android sin soporte. Es decir, no reciben actualizaciones.

El ranking está en:



Las versiones con soporte conjugan un 60.78%. El resto del share, casi un 40%, no poseen ya soporte oficial de actualizaciones:

Podríamos preguntarnos con legitimidad ¿Qué hacen esas versiones tan antiguas de Android aun en el mercado? Debemos tener presentes que muchos terminales Android con una larga vida aún siguen en funcionamiento en países con economías menos desarrolladas. Son terminales baratos con prestaciones humildes pero que aún cumplen una función básica para las personas de dichas regiones.

Otra gran parte de los terminales sin soporte oficial son teléfonos que todavía funcionan bien. Pensemos que Android 12, sin soporte, solo tiene algo más de tres años.

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-2025-21556	Oracle Agile PLM Framework	Permite control total del software a través de HTTP, fácilmente explotable de forma remota.	9,9
CVE-2025-21298	Windows OLE	Un atacante puede ejecutar código al enviar un correo malicioso a Outlook, incluso en vista previa	9.8
CVE-2025-21311	Windows NTLMv1	Explotable remotamente con baja complejidad, permite obtener privilegios de SYSTEM	9.8
CVE-2025-21524	Oracle JD Edwards EnterpriseOne Tools.	Permite ejecución de código sin autenticación	9.8
CVE-2025-29966	Windows RDP (cliente)	Permite ejecución de código arbitrario al conectar con un servidor RDP malicioso	8.8
CVE-2025-20188	Cisco IOS XE	Permite a atacantes remotos no autenticados subir archivos arbitrarios y ejecutar comandos como root mediante un JWT codificado de forma fija. Requiere que la función de descarga de imágenes fuera de banda esté habilitada	10
CVE-2025-20281	Cisco ISE e ISE-PIC	Permite a atacantes remotos no autenticados ejecutar comandos como root mediante explotación de la API, comprometiendo completamente el sistema	10
CVE-2025-22467	Ivanti	Permite a atacantes autenticados ejecutar código arbitrario y provocar corrupción de memoria en el sistema	9.9
CVE-2025-22457	Ivanti	Permite a un atacante tomar control total del sistema afectado. Está siendo explotada activamente	9.8
CVE-2024-55591	Fortinet	Permite a atacantes remotos obtener privilegios de superadministrador mediante solicitudes manipuladas. Explotación activa confirmada. (publicado el 14/01/2025)	9.6

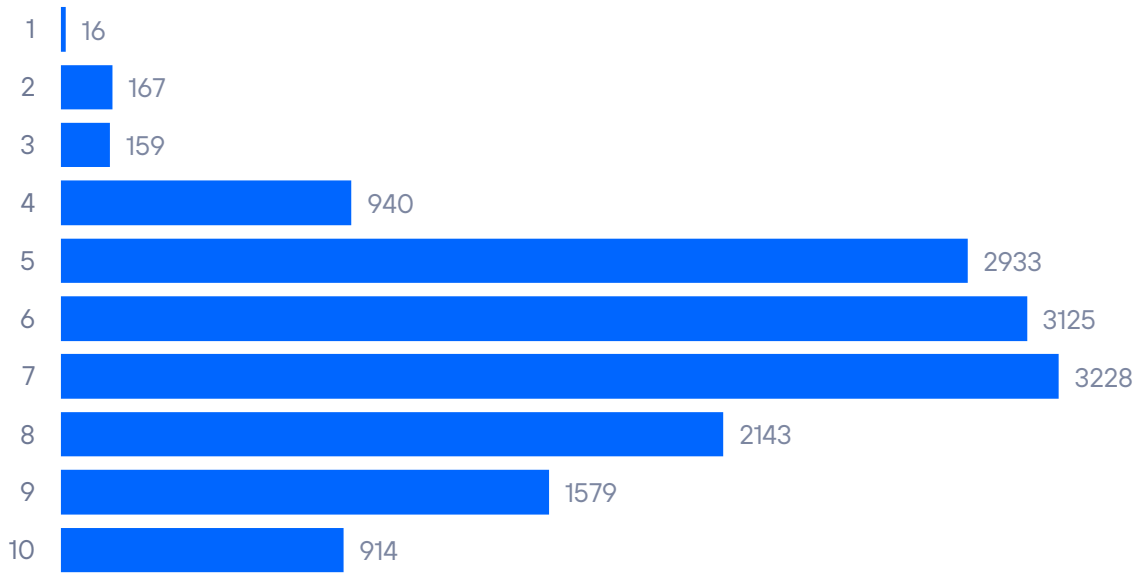
CVE-2025-20188	Cisco IOS XE	Permite a atacantes remotos no autenticados subir archivos arbitrarios y ejecutar comandos como root mediante un JWT codificado de forma fija	10
CVE-2025-1960	Schneider Electric SE	Vulnerabilidad de inicialización de un recurso con un valor predeterminado inseguro que podría provocar que un atacante ejecute comandos no autorizados cuando las credenciales de contraseña predeterminadas de un sistema no se hayan cambiado en el primer uso. El nombre de usuario predeterminado no se muestra correctamente en la interfaz WebHMI.	9.2
CVE-2024-54092	Industrial Edge Device Kit de Siemens	Aunque el Código CVE sea de 2024, la fecha de publicación es de abril-2025. La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto no autenticado eluda la autenticación y se haga pasar por un usuario legítimo.	9.3
CVE-2025-2567	XPort de Lantronix	Un atacante podría modificar o deshabilitar la configuración, interrumpir la monitorización de combustible y las operaciones de la cadena de suministro. Esto podría generar riesgos de seguridad en el almacenamiento y transporte de combustible.	9.3
CVE-2025-36535	ModBus Gateway de AutomationDirect	El servidor web integrado carece de autenticación y controles de acceso, lo que permite acceso remoto sin restricciones: cambios de configuración, interrupciones operativas o ejecución de código arbitrario...	10
CVE-2025-40585	Energy Services	Se ha identificado una vulnerabilidad en Energy Services (todas las versiones con G5DFR – un grabador multifuncional capaz de grabar y almacenar todas las formas de onda eléctrica). Las soluciones afectadas contienen credenciales predeterminadas.	9.5
CVE-2025-6029	Automotive Security Research Group (ASRG)	Uso de códigos de aprendizaje fijos, uno para bloquear el vehículo y otro para desbloquearlo, en el transmisor de llavero del sistema de entrada sin llave inteligente genérico de posventa de KIA	9.4

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.

RIESGO DE LAS VULNERABILIDADES

Distribución de vulnerabilidades por riesgo

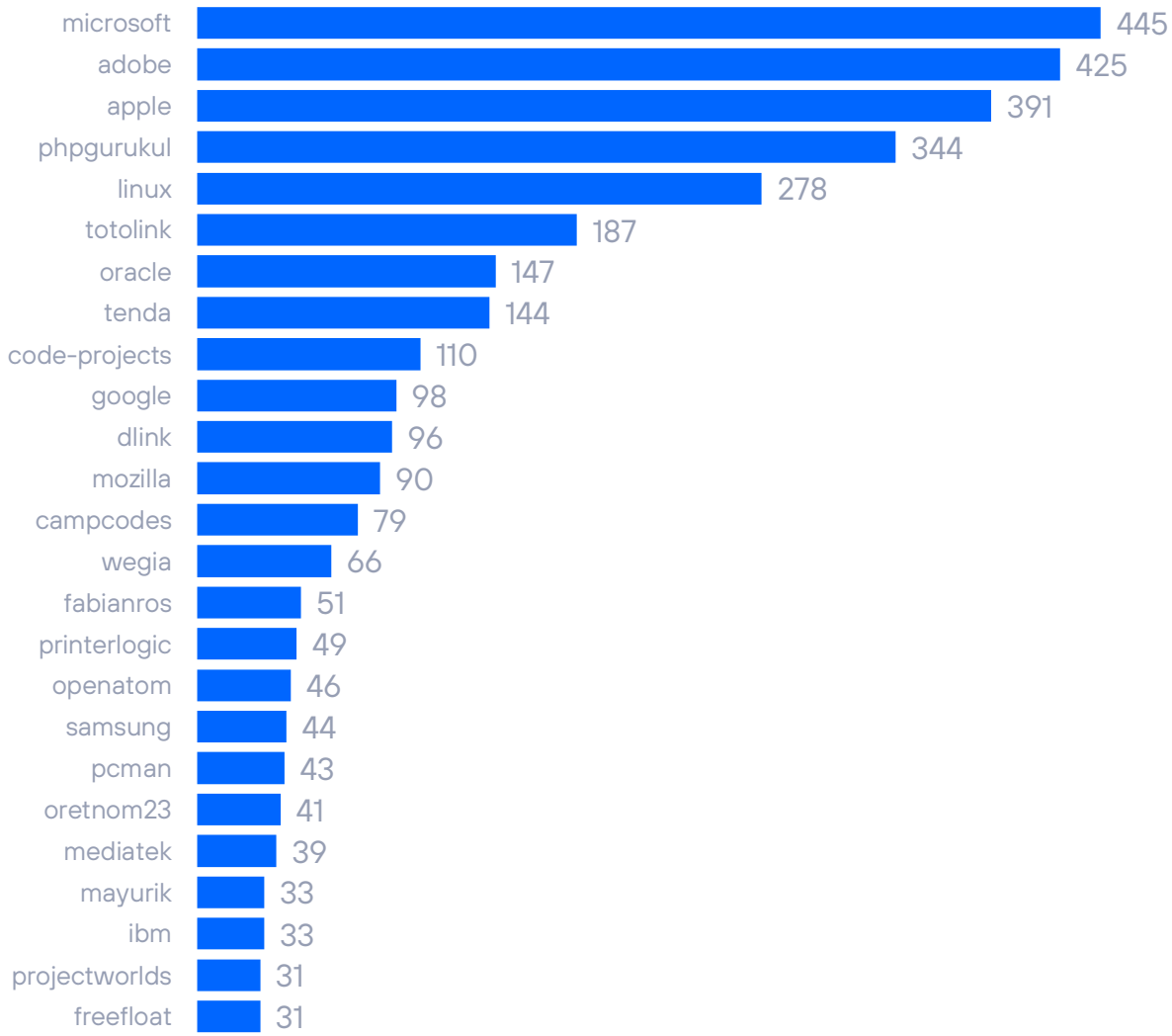


Top 25 compañías con más CVE acumulados

Durante el primer semestre de 2025, Microsoft lidera por número de vulnerabilidades conocidas, seguido de Adobe y Apple. En general, es habitual que Microsoft, Adobe, Google y Oracle estén siempre entre los primeros en número de vulnerabilidades. Linux, tras situarse muy por encima el semestre pasado (la razón la explicamos en esta entrada de blog: Linux y la paradoja de las vulnerabilidades: más reportes, ¿más seguridad?) ocupa ahora la cuarta posición.

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 2025

APT28 – Fancy bear: El perejil de todas las salsas.

Mucha experiencia y mucha actividad en lo que llevamos de 2025. Los han pillado en operaciones de inteligencia utilizando la técnica de ingeniería social de "Clickfix".

Los hemos visto acusados por el Ministerio de Asuntos Exteriores de Francia de haber atacado al menos a una docena de entidades francesas en los últimos años.

Los hemos visto ejecutando una campaña de ciberespionaje denominada "RoundPress", explotando 0-day para acceder a servidores de correo de organizaciones gubernamentales de varios países.

Los hemos visto atacando entidades de defensa, transporte, TI, tráfico aéreo y marítimo en varios países europeos y en EE.UU. con un elemento común: estaban dando servicios a Ucrania.

Y todo esto... en 6 meses ¿Qué nos deparará el siguiente semestre?

Más información en https://www.bleepingcomputer.com/tag/apt28/

Lazarus: Se levanta, anda... y triunfa

Lazarus es uno de los APT Group más conocidos en el ecosistema de la ciberseguridad. No en vano, son parte importante de la financiación de quien los patrocina.

En este caso, y a pesar de tratarse de un semestre agitado, vamos a comentar en concreto una comunicación del FBI. En ella se confirma que los ladrones del Exchange Bybit, donde se robaron 1.500 millones de dólares, era este grupo. Lazarus logró vulnerar una de las carteras frías, consideradas teóricamente más seguras, para conectarla a una billetera caliente, acceder a los fondos y dividirlos en múltiples billeteras (y criptoactivos) para dificultar su rastreo.

Según la BBC, parte del programa de misiles norcoreano se habría financiado a través del robo de criptoactivos.

Más información en: https://www.ic3.gov/PSA/2025/PSA250226

Primitive Bear: primitivo, pero muy listo

Este oso primitivo ha evolucionado y ha montado una infraestructura para desplegar malware utilizando túneles usando el servicio de pruebas de TryCloudflare. Esta táctica no es nueva y ya fueron detectados empleándola en septiembre de 2024.

Sin embargo, la cabra tira al monte y el oso a su estado primitivo. Los investigadores califican a este oso como poco sofisticado, ya que deja bastante rastro y realiza acciones redundantes, como desplegar varias puertas traseras o downloaders.

Sin embargo, lo que tienen de poco sofisticados lo compensan con el trabajo. Tienden a actualizar y cambiar los métodos de ofuscación de sus herramientas para evitar ser neutralizados.

Más información en: Hackers Leveraging Cloudflare Tunnels, DNS Fast-Flux to Hide GammaDrop Malware

Mythic Leopard: El gato que maneja las ratas

Esto va de RATS.

Concretamente, de los que despliega este grupo atacando a empresas de varios sectores de la India: Xeno RAT, Spark RAT y una nueva detección: CurlBack RAT

Ferrocarriles, petróleo y gas... es un gran paso para alguien que se encargaba principalmente de universidades y grupos de investigación. Una vez dentro, capturan toda la información que pueda tener valor.

APT36, como también se los conoce, se centra principalmente en los sistemas Linux, mientras que otros grupos "hermanos" se centran en sistemas Windows.

Más información en: https://thehackernews.com/2025/04/pakistan-linked-hackers-expand-targets.html

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

El caso más relevante de este semestre ha sido (y sigue siendo) una intrusión de la que hicimos un análisis inicial en este artículo de marzo. Por resumirlo brevemente, a principios de año, un atacante consiguió vulnerar uno de nuestros señuelos (sector oil&gas) a través de la bahía de ingeniería. Una contraseña robusta y medidas de seguridad típicas en los entornos industriales reales (porque de eso va Aristeo, recordémoslo) no fueron suficientes para detenerlos. Del vector de entrada, de momento, no vamos a comentar nada.

Tras esta intrusión inicial, el atacante cambió su forma de actuar. Digamos que se volvió más "novato", por lo que vimos claramente que se trataba de otro atacante. La actividad dentro de la máquina se ceñía a acciones menores y poco sofisticadas contra objetivos concretos. Incluso se dejaron un documento con una lista de objetivos y un software de escaneo de puertos en la papelera de reciclaje...

Tras la primera intrusión, hicimos lo que cualquiera haría en nuestro caso: los dejamos jugar. Conservamos cierto mantenimiento, que ellos podían ver, pero no queríamos tocar demasiado. Hasta que, hace un mes, hicimos una limpieza profunda e, incluso, cambiamos la contraseña (17 caracteres aleatorios con todo el pack de símbolos, números...). Por fin, pensarían ellos, "el de sistemas se ha enterado de algo". No nos interesaba el segundo atacante, aunque nos dio buena información. Nos interesaba el atacante de altas capacidades. Por eso, aprovechamos para desplegar aún más capacidades de captura de información y ver qué pasaba.

Una semana más tarde en la que los atacantes con menos conocimientos no podían acceder, el atacante profesional volvió a aparecer y... volvió a entrar. Seguimos guardándonos el vector de entrada hasta que podamos hacer más comprobaciones y estudios. Este atacante volvió a persistir el acceso, y alguien del equipo B (sospechamos) cambió la contraseña del RDP, por lo que "perdimos" el acceso a la máquina.

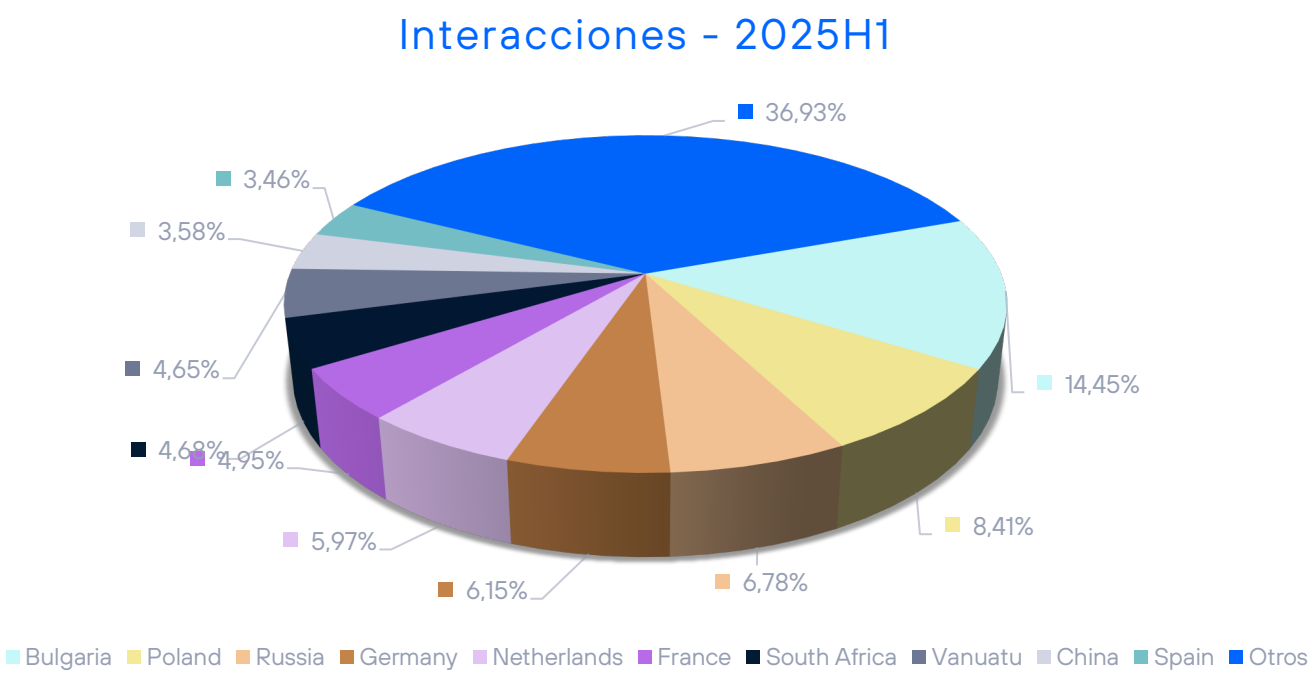
En ese momento, desconectamos la máquina y volvimos a actuar. Ya hemos capturado suficiente información y no podemos permitir que una máquina quede secuestrada y al albur de un atacante.

Por cierto, respecto a los orígenes de los atacantes, es curioso ver cómo se trata de direcciones IP con poca actividad y que, de hecho, no están registradas en un 99% en otros motores de inteligencia y fuentes de información de las más consultadas en Internet. Esto, junto con otra información, nos ha llevado a deducir que el atacante es un APT-Group y que no está alquilando el acceso a terceros. Se trata de un "Equipo A" que posee una capacidad y conocimientos muy altos y un "Equipo B" que se dedica al "menudeo", por así decirlo.

Una última cosa, aunque hayamos capturado suficiente información y cerrado el acceso a la máquina, tenemos planes. Stay tuned.

Pasamos a la estadística general de la información registrada. En el primer semestre de 2025 se detectaron casi 82 millones de eventos de ciberseguridad. Llegados a este punto, conviene recordar que se trata de eventos complejos, y que, gracias a Aristeo 2.0, los eventos ahora se asocian entre sí, lo que convierte los más de 369 millones de eventos "simples" que hemos tenido en esa cifra de 82. Con todo, podemos calcular el aumento respecto al semestre pasado, que fue del 11%. Comparando las cifras obtenidas con el primer semestre de 2024 supone un ascenso de casi el 18%

La distribución por países sería la siguiente:

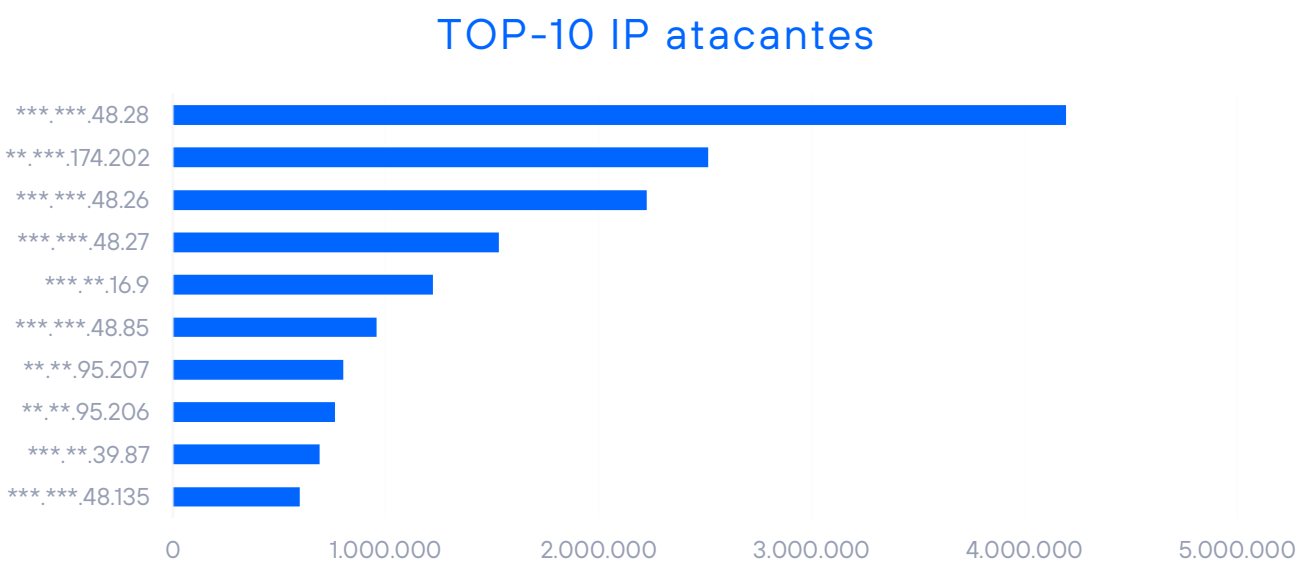


Este semestre, el top-10 lo encabeza Bulgaria, viejo conocido respecto a los orígenes que siempre nos visitan en gran número. La dispersión, por otra parte, es muy similar al semestre pasado.

Ahora vamos a ver las diez direcciones IP con más interacción con el sistema de Aristeo. En este semestre, los países con más visitas a Aristeo son los que posicionan sus IP en la lista. En este caso, se podría hablar de cierta estabilidad.

De igual forma que durante el anterior semestre, la gran mayoría de direcciones IP de este Top-10 proviene del centro-norte-este de Europa. La diferencia respecto al H2 de 2024 es que, en este caso, el 100% de las direcciones en el Top-10 es de esta región del mundo (el 85% el semestre anterior). Además, el Top-10 representa casi el 19% sobre el total de orígenes detectados por Aristeo.

Para ver la magnitud, podemos ver el contexto concreto: casi 2 millones de eventos de cada 10 millones registrados, pertenecen al Top-10 de IP, y son todas de Europa. Y así hasta 82 millones de eventos complejos.



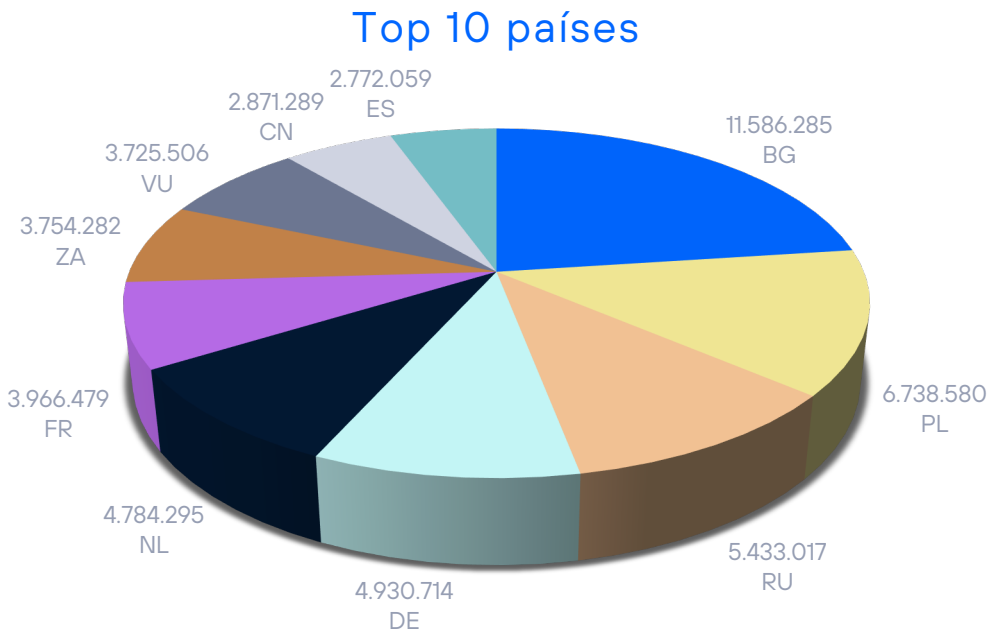
A continuación, vemos cómo se reparten el *top 10* de los países registrados. En este semestre vuelven los orígenes españoles y aparecen dos nuevas estrellas: Sudáfrica y Vanuatu. Seguramente, todos sabemos situar Sudáfrica en un mapa (aunque sólo sea por las pistas que da el nombre). Pero Vanuatu... el archipiélago de Vanuatu, al este de Australia, está compuesto por 12 islas grandes y 70 islotes. Tiene una población similar a Lugo y Orense, y viven allí (según el Ministerio de Exteriores de España) 3 españoles**.**

Después de la lección de geografía (nunca está de más aprender algo nuevo) no hemos encontrado un patrón claro por el cual este país se haya colado como octavo en la lista de países de origen con más interacciones contra la red de Aristeo. Sólo podemos justificarlo a través de dos razonamientos.

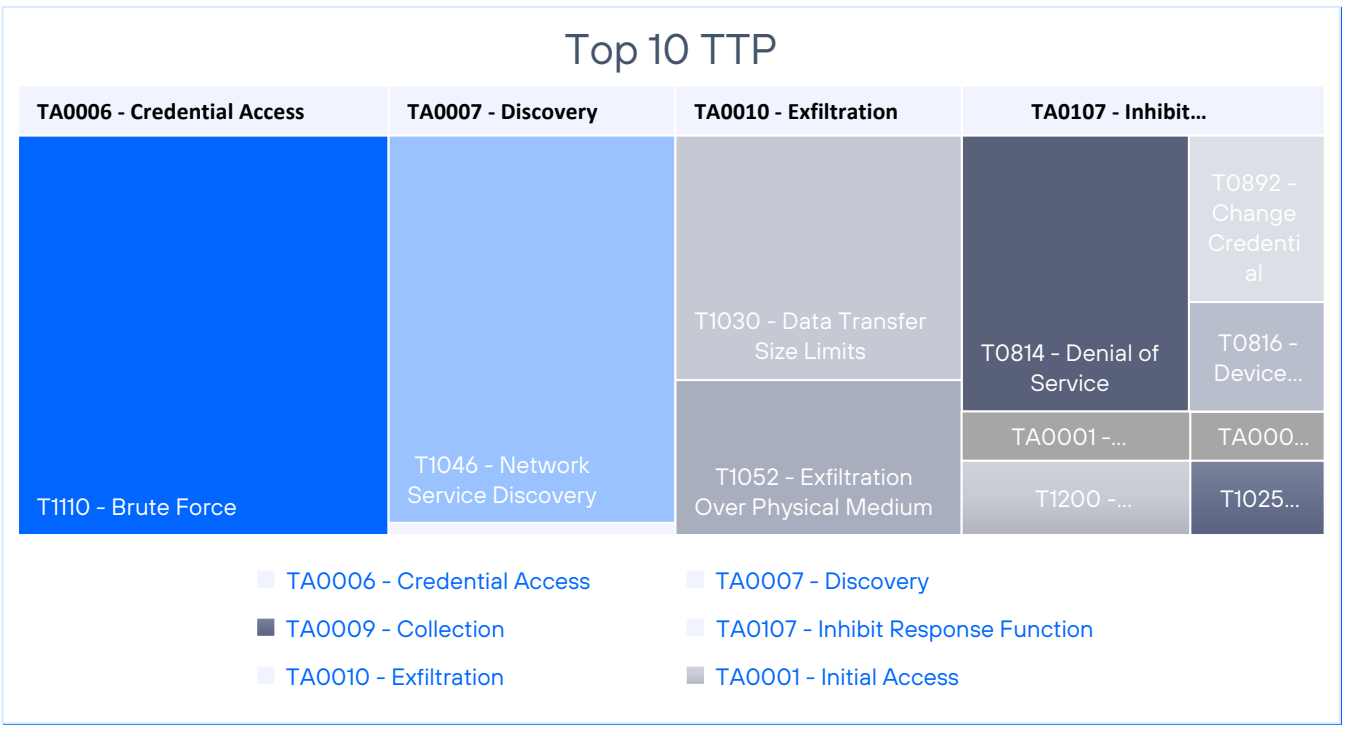
- En el semestre anterior comentamos que habíamos abierto sedes de Aristeo fuera de Europa y quizás esa deslocalización tenga que ver con el interés de otros atacantes que tienen en cuenta la región del mundo en la que despliegan su actividad. De hecho, esto es algo que ya vimos y comentamos en el anterior informe:

De nuevo, el hecho de deslocalizar más Aristeo implica menor foco en un punto concreto de la geografía mundial y más aprovechamiento respecto al resto.

- Otra razón que puede influir es que Vanuatu se está poniendo de moda. Es un país sin impuestos personales y con un programa de ciudadanía en el que con "poco" dinero y 3 meses se otorga a cualquier extranjero que cumpla con las condiciones. Este aspecto, que puede parecer banal a primera vista, proporciona el 30% del PIB del país por la cantidad de personas que se están "mudando". Este tipo de situaciones afectan en el panorama económico y también en el panorama cibernético. No es el primer país relativamente pequeño que vemos pasar por el Top-10 de Aristeo. Antes han pasado Belice (varias veces), Panamá...



Este semestre, gracias a Aristeo 2.0, incorporamos un nuevo gráfico con las TTP más explotadas por los atacantes.



Se puede observar que la mayor parte de la actividad se centra en acciones iniciales, como el intento de acceso a través de fuerza bruta. Otras acciones como el descubrimiento, la exfiltración, la recolección de información... son menores porque los señuelos de Aristeo no son una barra libre. Como buen entorno de Deception, los señuelos están debidamente configurados y sólo atacantes con un nivel alto pueden acceder y seguir demostrando sus TTP. Respecto a las referencias a medios físicos, los entornos de Aristeo no suelen estar físicamente al alcance de nadie, pero sí que se pueden usar como entornos de aprendizaje para sus empleados, o poner como cebo si el cliente quiere detectar posibles insiders.

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: 335.637 direcciones IP, 146.329 dominios y 297.615 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	185119	62,20%
Phishing	95977	32,25%
Lumma Stealer	5613	1,89%
Formbook	4559	1,53%

Clearfake	851	0,29%
FAKEUPDATES	695	0,23%
DCRat	537	0,18%
Stealc	291	0,10%
Vidar	290	0,10%
Coper	272	0,09%

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.

En la pasada edición teníamos como malware estrella el Stela Stealer. Desaparece pero en su lugar viene Lumma Stealer golpeando fuerte, además con idéntica funcionalidad: robar datos. Afecta a sistemas Microsoft Windows y emplear sobre todo el vector phishing a través de correos electrónicos.

Le acompaña en el ranking FormBook, otro stealer disfrazado de troyano que además de Windows también posee una versión MacOS.

El resto se reparte, como vemos, por las familias de malware más diseminadas. Infraestructura que les sirve como punto de descarga, captación de ordenes e incluso para depositar temporalmente información robada. Una larga cola de familias con distinto ADN pero con el común de su carga maliciosa.

¿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).

vercel.app	10281	3,45%
webflow.io	9480	3,19%
github.io	6892	2,32%
pages.dev	4940	1,66%
github.com	3448	1,16%
weebly.com	2325	0,78%
godaddysites.com	1913	0,64%
duckdns.org	1519	0,51%
r2.dev	1319	0,44%
glitch.me	1154	0,39%

Como es habitual, los primeros puestos pertenecen a servicios online que permiten alojar de forma gratuita contenido web: vercel.app, weflow.io, github.io.

Es un patrón común: ¿Para qué arriesgarse en alojamiento privado o en servidores comprometidos cuando te ofrecen alojamiento gratuito y anónimo?

También existen dominios asociados a estas URL maliciosas que usan resolvedores de dominios dinámicos: duckdns.org. Es decir, en realidad son IP desnudas que mediante un servicio gratuito de DNS pueden ser resueltas a un subdominio particular e incluso si necesitan migrar la infraestructura maliciosa, la mueven de dirección IP y seguirán resolviendo a la nueva localización.

Como vemos, tanto en un tipo de servicio como en otro la tónica es siempre: gratuito y anónimo. Dos características que son buscadas y empleadas con ahínco por los cibercriminales.

¿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.

India	68265	20,34%
Estados Unidos	52462	15,63%
China	30877	9,20%
Singapur	17491	5,21%
Vietnam	16084	4,79%
Rusia	13246	3,95%
Alemania	11178	3,33%
Brasil	8914	2,66%
Reino Unido	7091	2,11%
Pakistan	6855	2,04%

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?

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:

Suspicious host	158322	47,17%
Mail Spammer	143953	42,89%
HTTP Spammer	117679	35,06%
Malicious host	81556	24,30%
Bruteforce	59340	17,68%
Hacking	57975	17,27%
Port Scanner	55216	16,45%
SSH Attacker	54335	16,19%
Proxy	51675	15,40%
HTTP Attacker	42955	12,80%

Coronando el ranking del top 10 encontramos una categoría generalista: "Suspicious host". Es una categorización que prácticamente solapa la mitad del conjunto de datos dado que se otorga siempre que existen indicios de actividad sospechosa aunque no se sabe aún con detalle la operativa observada desde esa dirección IP.

Más adelante, cuando se le suma una etiqueta con el detalle del porqué: spam, escaneos indiscriminados, etc, la etiqueta de host sospechoso no se retira dado que se trata de un refinamiento posterior. Otro tipo de etiquetado generalista lo encontramos en "Malicious host". Idéntico significado, aunque agrega algo más de certeza en el diagnóstico preliminar.

Si realizamos una agregación de etiquetas por actividad concreta de las direcciones IP, vemos que el SPAM, tanto en su vertiente HTTP como Mail, coronan el ranking con más de un 80% de etiquetas. Recordemos, las etiquetas se solapan por lo que una misma IP puede contener varias de ellas. Por ejemplo, una generalista de "sospechosa" y "HTTP Spammer", e incluso que la misma IP sirva para escanear puertos porque haya sido una actividad detectada en algún momento dado.

SSH Attacker es una categoría singular. Con casi total acierto, pertenece a grupos de hosts infectados y coordinados por una botnet del tipo Mirai. El escaneo masivo en busca de accesos fáciles vía SSH (Secure Shell) es una constante desde hace décadas en Internet (como lo fue en sus inicios Rlogin o telnet). Casi un 16,19% de las direcciones IP han sido observadas realizando ataques sobre SSH (la mayoría ataques por diccionario sobre el login).

De forma parecida, "Bruteforce" se refiere al continuo intento de realizar una autenticación por fuerza bruta (en realidad, de nuevo: diccionarios de nombre de usuario y contraseñas comunes). Esta categoría suma un casi 17,68%.

En otra subcategoría, escaneos indiscriminados, encontramos: Port y Host escáner. Direcciones IP que han sido detectadas realizando escaneos masivos a rangos completos o múltiples puertos en determinados hosts. Es decir, escaneos horizontales buscando ciertos puertos o verticales (en profundidad) en un grupo de hosts.

La categoría "Proxy" con casi un 15,4% son sistemas que, ya sea de forma adrede o insospechada, sirven de puerta de acceso o salto (hop) a otras máquinas para esconder el origen de ciertos ataques o accesos no autorizados.

De forma general, encontramos la categoría "hacking" con un 17,27% cerrando el ranking. Son nodos que han sido observados realizando ataques en general, ya sea intentando encontrar vulnerabilidades SQL o lanzando exploits. A menudo, se trata de escáneres de vulnerabilidades usados de manera indiscriminada y, por supuesto, sin autorización.

¿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:

xyz	43193	29,52%
com	34609	23,65%
io	9768	6,68%
top	5170	3,53%
org	4705	3,22%

app	4188	2,86%
net	3532	2,41%
dev	2896	1,98%
shop	2450	1,67%
gg	1831	1,25%

"xyz" corona este semestre nuestro ranking de TLDs. Aunque se disputa en alternancia el liderato con "com", sube con fuerza y le arrebata el testigo. "xyz" nació en 2014 y fue impulsado por Google por hacer el juego con su matriz: "abc.xyz".

¿Por qué "xyz" es el "favorito" de los creadores de malware? Por sus precios competitivos: desde 0.99$ por año es una cifra más que atractiva para emplear dominios de este TLD.

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.

"gg" que se nos cuela en el top 10 es un TLD geográfico que pertenece a Guernsey. Una isla en el Canal de la Mancha, perteneciente a Reino Unido. Es un TLD asociado ultimamente a sitios de videojuegos y e-sports.

¿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	44483	30,40%
Metastealer	39659	27,10%
Formbook	14389	9,83%
Lumma Stealer	8623	5,89%
Virut	6708	4,58%

Malware Download	5077	3,47%
Joker	2394	1,64%
Xworm	1734	1,19%
BumbleBee	1608	1,10%
Bankbot	1406	0,96%

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 en general. El resto, pertenecen a familias de malware que han tenido repercusión.

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

La verdad sobre los 320 segundos para hackear Bitcoin: un análisis técnico

Análisis de una intrusión en la plataforma Aristeo como ejemplo de sus capacidades predictivas

Linux y la paradoja de las vulnerabilidades: más reportes, ¿más seguridad?

INTELIGENCIA ARTIFICIAL

El increíble mundo interior de los modelos de lenguaje LLM (I)

El increíble mundo interior de los modelos de lenguaje LLM (II)

La tokenización y el caballero andante Don Quijote