Telefónica Tech

Informe sobre el estado de la seguridad 2025 H2

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

Índice

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.

En la segunda mitad de 2025, la ciberseguridad vivió dos acontecimientos que nos parecen relevantes. En septiembre de 2025, un colectivo de atacantes autodenominado *Scattered LapSus Hunters* lanzó una amenaza inusual contra Google: exigió que la compañía despidiera a dos miembros de su Threat Intelligence Group bajo la advertencia de filtrar supuestos datos internos de Google si no accedía a sus demandas. Los atacantes no presentaron pruebas claras de tener acceso real a sistemas internos, y la amenaza, probablemente, no era más que una bravuconada. Sin embargo, esta táctica da que pensar sobre el futuro de la extorsión. La presión psicológica sobre los técnicos (de los que se ofrecieron nombres y apellidos) y la presión reputacional contra profesionales de ciberseguridad en lugar de (solo) exigir dinero por datos. ¿Llegarían en un futuro a desincentivar las investigaciones en curso a través de esta diana virtual sobre los técnicos reputados? Habrá que estar atento a esta nueva maniobra, que abre la puerta a debilitar la respuesta organizativa y sembrar miedo o desconfianza hacia los equipos de investigación.

Por otro lado, algunos días después Anthropic describió el primer ciberataque orquestado casi totalmente por IA. Se considera el primer gran ciberataque llevado a cabo en gran parte por una inteligencia artificial con mínima supervisión humana.

Según el reporte, un grupo cibernético patrocinado por un Estado manipuló a Claude, para ejecutar tareas ofensivas de manera autónoma. El modelo fue "engañado" para realizar la mayor parte del trabajo (desde reconocimiento de sistemas, generación de código de explotación, hasta recolección de credenciales y extracción de datos) con muy poca intervención humana. Se supone que se cruzó una línea: las IA ya no se limitan a asistir a atacantes con sugerencias o automatizaciones parciales, sino que pueden orquestar campañas complejas por sí mismas, llevando la velocidad y escala de los ciberataques a un nuevo nivel.

Sin duda los atacantes están aprovechando lo mejor de todos los mundos, sin regulaciones ni cortapisas. La extorsión no solo a empresas, sino a investigadores. Algo inaudito, que esperamos que quede en la anécdota. Y el aprovechamiento de herramientas infinitamente potentes como la IA, doblegada a sus intereses, para desarrollar más ataques, más potentes en mucho menor tiempo. Potencialmente demuestra que se pueden llevar los ataques a otro nivel de intensidad y profundidad con muy pocos recursos.

Los atacantes son cada vez más audaces en su objetivo de socavar tanto las defensas tecnológicas como la moral de quienes las mantienen. Simplemente porque pueden.

Tanto si se es aficionado como profesional, es importante ser capaz de seguir el ritmo de las noticias relevantes sobre ciberseguridad: ¿qué es lo más relevante que está pasando? ¿Cuál es el panorama actual? El lector dispondrá con este informe de una herramienta para comprender el estado de la seguridad desde diferentes perspectivas, y podrá conocer su estado actual y proyectar posibles tendencias a corto plazo. La información recogida se basa en buena parte en la recopilación y síntesis de datos internos, contrastados con información pública de fuentes que consideramos de calidad. ¡Allá vamos!

LOS INCIDENTES MÁS DESTACADOS DEL SEGUNDO SEMESTRE DE 2025

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

JULIO

- La **FIA** es una asociación internacional sin ánimo de lucro que coordina numerosos campeonatos de automovilismo, incluyendo la Fórmula 1 y el Campeonato Mundial de Rally (WRC). La FIA (Fédération Internationale de l'Automobile), **afirmó que atacantes accedieron a datos personales tras comprometer varias cuentas de correo electrónico** tras un ataque de phishing.
- Investigadores de ESET **descubrieron que RomCom estaba explotando una vulnerabilidad 0-day en WinRAR descubierta el 18 de julio de 2025** y notificó al equipo detrás de la popular herramienta de archivado. ESET cree que la vulnerabilidad se utilizaba para extraer ejecutables peligrosos a rutas de ejecución automática cuando un usuario abre un archivo especialmente diseñado. La vulnerabilidad era similar a otro problema de recorrido de ruta en WinRAR, revelada un mes antes e identificada como CVE-2025-6218.
- La empresa estatal de defensa francesa, Naval Group, anunció que estaba investigando un ciberataque después de que **1 TB de datos supuestamente robados se filtraran en un foro de fugas de información.** La compañía calificó esto como un "intento de desestabilización" y un "ataque a la reputación", a lo que respondió presentando una denuncia para proteger los datos de sus clientes. El 23 de julio de 2025, un actor de amenazas conocido como "Neferpitou" publicó una gran muestra de 13 GB de datos presuntamente robados de Naval Group. Los datos contenían lo que parece ser un CMS clasificado para buques militares, documentos técnicos, máquinas virtuales de desarrollo con datos de simulación y comunicaciones internas.

AGOSTO

- **Nissan Creative Box,** el brazo creativo del fabricante multinacional japonés de automóviles, **fue atacado por ransomware y perdió numerosos datos sensibles en el incidente.** La empresa es un estudio especializado en diseño de satélites que forma parte de la red global de diseño de Nissan.
- Google reconoció que **había sufrido un ciberataque que supuso la filtración de datos de clientes de Google Ads.** Aunque la empresa no indicó cuántos clientes se habían visto afectados, los atacantes, "Sp1d3rHunters" indican que **recogieron aproximadamente 2,55 millones de registros.** El ataque fue dirigido contra el CRM de Salesforce y la compañía había detectado previamente una campaña de phishing y vishing contra varios de sus empleados.
- El Poder Judicial Federal de **Estados Unidos confirmó que había sufrido un ciberataque a sus sistemas de gestión electrónica de casos que albergan documentos judiciales confidenciales.** La organización afirmó que, si bien la mayoría de los documentos en el sistema son públicos, ciertos archivos sellados contienen información confidencial que ahora está protegida con controles de acceso más estrictos destinados a bloquear a los atacantes.
- **Investigadores de Nextron Systems descubrieron un malware para Linux que había evadido la detección durante más de un año,** permitiendo a los atacantes obtener acceso SSH

persistente y eludir la autenticación en sistemas comprometidos. El malware explota la infraestructura de autenticación PAM (Pluggable Authentication Modules), contaba con técnicas de ofuscación, capacidades anti depuración, cifrado y limpiaba el entorno de ejecución de cualquier rastro de actividad maliciosa.

SEPTIEMBRE

- **Asahi Group Holdings, Ltd (Asahi), el grupo responsable de la cerveza más vendida de Japón**, **notificó un ciberataque que interrumpió varias de sus operaciones. Según la empresa, el incidente afectó a su actividad de pedidos y envíos, que fueron completamente suspendidos.** Las operaciones del centro de atención telefónica y el mostrador de atención al cliente también quedaron inaccesibles. Asahi posee aproximadamente un tercio de la cuota de mercado nacional. Emplea a 30.000 personas, produce 100 millones de hectolitros de bebidas y, en 2024, la empresa reportó unos ingresos anuales de casi 20.000 millones de dólares estadounidenses.
- El equipo Google Threat Intelligence Group (GTIG) **detectó un malware denominado "Brickstorm" que ha permanecido activo 393 días de media en sus víctimas.** Los investigadores confirmaron que, entre las organizaciones comprometidas, se encuentran los sectores legal y tecnológico, proveedores de software como servicio (SaaS) y también subcontratistas de procesos de negocios (BPO).
- **Google publicó su sexto parche del año contra una vulnerabilidad 0-day en Chrome etiquetada como explotada.** En perspectiva, en septiembre de 2024 la cifra fue de 10 parches publicados con las mismas características
- **Microsoft y Cloudflare desarticularon una operación masiva de phishing como servicio (PhaaS), conocida como RaccoonO365,** que ayudó a los ciberdelincuentes a robar miles de credenciales de Microsoft 365. El grupo de ciberdelincuentes detrás de este servicio (también rastreado por Microsoft como Storm-2246) **robaron al menos 5.000 credenciales de Microsoft de 94 países desde al menos julio de 2024,** utilizando kits de phishing RaccoonO365 que incluían páginas CAPTCHA y técnicas anti-bot para parecer legítimos y evadir el análisis.

OCTUBRE

- **Un actor extranjero se infiltró en el Campus de Seguridad Nacional de Kansas City** de la Administración Nacional de Seguridad Nuclear a través de vulnerabilidades en la aplicación basada en navegador SharePoint de Microsoft, **lo que generó preguntas sobre la necesidad de consolidar más protecciones de seguridad de IT/OT a nivel federal.**
- **El 6 de octubre, la botnet "Aisuru" alcanzó el pico máximo registrado en la historia de un ataque DDoS: 29.69 Tbps.** El ataque fue dirigido contra varias plataformas de juegos online. Esta misma botnet, basada en Mirai y que se basa en infectar dispositivos IoT, ha sido utilizada para ejecutar otros ataques a gran escala, como los 22.20 Tbps que registró y mitigó Cloudflare y los 15.72 Tbps registrados por Azure y que fueron dirigidos contra una única IP en Australia
- **España desmanteló al grupo de cibercriminales "GXC Team" y detuvo a su líder, un brasileño de 25 años conocido como "GoogleXcoder".** El equipo de GXC, muy activo en España, operaba una plataforma de crimen como servicio (CaaS) que ofrecía kits de phishing

impulsados por IA, malware para Android y herramientas de estafa de voz a través de Telegram y un foro de atacantes de habla rusa. **El análisis de los dispositivos incautados en las detenciones iniciales (practicadas en 6 ciudades de toda España) llevó más de un año debido a la complejidad y extensión del grupo de cibercriminales.**

NOVIEMBRE

- **Sistemas de alerta de emergencia en todo Estados Unidos interrumpidos tras el ciberataque OnSolve CodeRED,** una plataforma en la nube de eventos críticos y notificaciones masivas. Dicha plataforma sufrió recientemente un ciberataque que le obligó a desconectar su entorno, **además de perder datos sensibles e incluso un cliente empresarial. OnSolve es un servicio que ayuda a las organizaciones a enviar alertas y comunicaciones urgentes por SMS, teléfono, correo electrónico, notificaciones push y más.** Es utilizado por gobiernos estatales y locales, como la policía y otros servicios de emergencia.
- **Un equipo de investigación encontró miles de credenciales, claves de autenticación y datos de configuración relacionados con organizaciones en sectores sensibles dentro de servicios en línea de embellecimiento de código ("Codebeauty")** y maquetadores de formato (por ejemplo, formateadores de JSON). Estos servicios incorporan la capacidad de almacenar para compartir el código a través de una URL generada pseudo-aleatoriamente y no indexada. El punto crítico es que esas URL no están cifradas ni contienen otro mecanismo de autenticación, por lo que, adivinando la estructura de generación las URL, se puede acceder al contenido sin problema.

DICIEMBRE

- La Policía Nacional **detuvo en Barcelona a un presunto atacante de 19 años, acusado de robar e intentar vender 64 millones de registros obtenidos en brechas de seguridad en nueve empresas.** El ciberdelincuente accedió a nueve empresas diferentes donde obtuvo millones de registros personales privados que luego vendió en línea.
- **La Oficina Nacional de Investigación de la policía nacional de Corea del Sur** detuvo a 4 personas por **acceder a cámaras IP y vender vídeos íntimos en un sitio web extranjero.** Las personas detenidas no tenían relación entre sí. Una de ellas compartió material que afectaba a menores de edad. También se actuó contra los responsables de los sitios web en los que se colgó el contenido y contra los usuarios que accedieron a esos vídeos.
  Además, la policía se dirigió a aquellas víctimas a las que consiguió llegar para avisarlas, darles toda la información e intentar ayudarlas en lo posible.
- **MITRE publicó las 25 debilidades (CWE) más asociadas a las vulnerabilidades de 2025.** En el puesto 1 se encuentra Cross-site Scripting, que repite respecto a 2024, mientras que en los puestos 2 y 3 se encuentran SQLi y CSFR respectivamente, que ascienden una posición cada una al caer la escritura fuera de límites al 5º puesto.
- **Una vulnerabilidad en MongoDB es siendo explotada activamente, con más de 87000 instancias potencialmente susceptibles identificadas en todo el mundo.** La vulnerabilidad en cuestión es CVE-2025-14847 (puntuación CVSS: 8,7), permite a un atacante no autenticado filtrar de forma remota datos confidenciales de la memoria del servidor MongoDB.

MÓVILES

Apple iOS

De iOS 18 a iOS 26

¿Un salto cuántico? No, pero sí un cambio drástico en el lenguaje visual del sistema operativo de Apple.

El cambio de numeración, del que ya dimos un avance en la pasada edición de este informe, obedece a elementos puramente estéticos. Apple parece adoptar una cifra que suene más a 2026 que a años anteriores, dada la cercanía que se estaba dando de los números de versiones respecto al calendario.

Además del cambio de numeración, iOS estrena un nuevo look con abundancia de transparencias, modernización de iconos, etc. Más allá de la estética, vamos a centrarnos en las mejoras de seguridad que trae iOS 26.

Nuevo permiso para dispositivos conectados por cable: ahora podemos decidir si permitimos o no la conexión de dispositivos externos vía USB cuando el teléfono esté bloqueado. Las opciones son: preguntar siempre, preguntar solo para nuevos dispositivos no vistos antes, permitir solo si el dispositivo está bloqueado o permitir la conexión siempre.

Esto nos permite controlar qué y en qué condiciones se conectan elementos externos a nuestro teléfono. La utilidad más práctica desde el punto de vista defensivo es eliminar o paliar el riesgo de que conecten un dispositivo malicioso vía USB en nuestra ausencia.

Claves de intercambio poscuánticas en TLS 1.3: a partir de ahora, el intercambio de claves en comunicaciones cifradas se hará empleando algoritmos resistentes a la computación cuántica, lo que debería preservar las comunicaciones supuestamente capturadas en el presente de ataques criptográficos en el futuro, cuando, previsiblemente, la tecnología cuántica esté disponible para el público.

Asistente de recuperación: iOS 26 incluye una nueva característica que permite recuperar el dispositivo si detecta fallos en el proceso de inicio del sistema, evitando en lo posible el bloqueo del terminal si el proceso es abortado por errores.

Bloqueo de contactos: Se ha añadido una nueva sección en los ajustes de privacidad y seguridad para la gestión de contactos bloqueados.

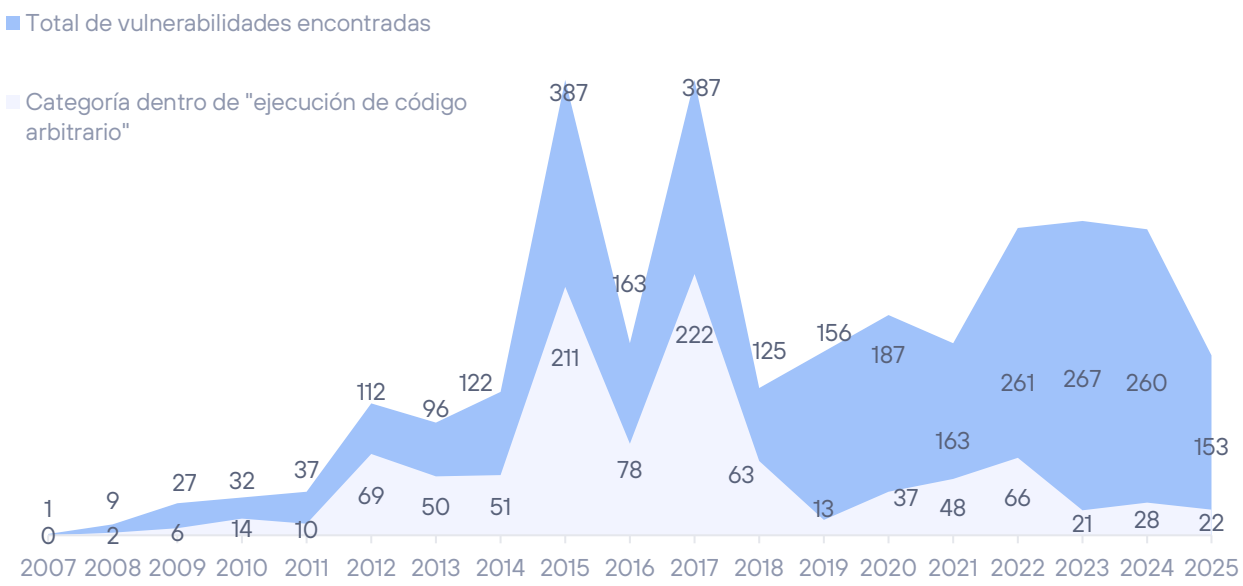
Los contactos bloqueados o no deseados pasan a ser tratados como un conjunto compartido entre ciertas aplicaciones y el sistema, es decir: contactos clasificados como spam telefónico o números desconocidos. Una característica que trata de alivia el problema de las llamadas no deseadas.

Evolución de vulnerabilidades en iOS durante el segundo semestre de 2025

El primer semestre de 2025 se cerró con 153 vulnerabilidades parcheadas, cuatro consideradas de alto riesgo, con posibilidad de ejecutar código arbitrario.

Un número similar al del segundo semestre de 2025, que lo supera con un buen margen: 178 parches.

VULNERABILIDADES EN IOS:
Evolución de vulnerabilidades por año



Vulnerabilidades y versiones publicadas en el segundo semestre de 2025

Tuvimos que esperar hasta finales de julio para que iOS 18.6 viese la luz. La sexta iteración venía con un lote de 32 parches de seguridad, muchos de ellos corrupciones de memoria que podrían causar la terminación repentina de la aplicación o fugas de información entre otras causas. No posee vulnerabilidades significativas o que recaben cierto protagonismo. Quince días después se publica 18.6.1 sin ningún parche de seguridad.

El 20 de agosto es publicada la 18.6.2. Es un parche de emergencia. El CVE-2025-43300 está siendo explotado activamente y además lo hace en objetivos específicos, tal y como apunta el propio informe de Apple. Se trata de un error en el control de escritura fuera de límites de un búfer de memoria durante el procesamiento de imágenes en el componente ImageIO. Un mes relativamente tranquilo.

Septiembre abre la temporada estrenando la nueva numeración. El 15 de septiembre nace iOS 26 y no viene precisamente vacío en el apartado de seguridad, son 34 parches corrigiendo sendas vulnerabilidades. Paralelamente se publicó 18.7 corrigiendo 13. El mismo día, se liberan parches para CVE-2025-43300 en las versiones 15.8.5, 16.7.12; versiones en teoría sin soporte de seguridad desde marzo de este año, aunque suele ser habitual que se publiquen parches para versiones aun "vivas" si el impacto es especialmente grave.

Más adelante, el 29 de septiembre, se publica un parche para una vulnerabilidad que corrige una escritura fuera de límites en un búfer al procesar fuentes de texto. Con el CVE-2025-43400 aparecen las versiones 18.7.1 y la primera actualización de iOS 26, la 26.0.1.

Y aunque octubre es el mes de Halloween, irónicamente no se publica ninguna actualización de seguridad, un mes atípicamente tranquilo, sin tratos ni sustos.

Noviembre nos deja de forma temprana la primera gran actualización de iOS 26, la 26.1. Sale con nada más y menos que 61 parches de seguridad. Le acompaña la nueva iteración para iOS 18, la 18.7.2, con 38 parches.

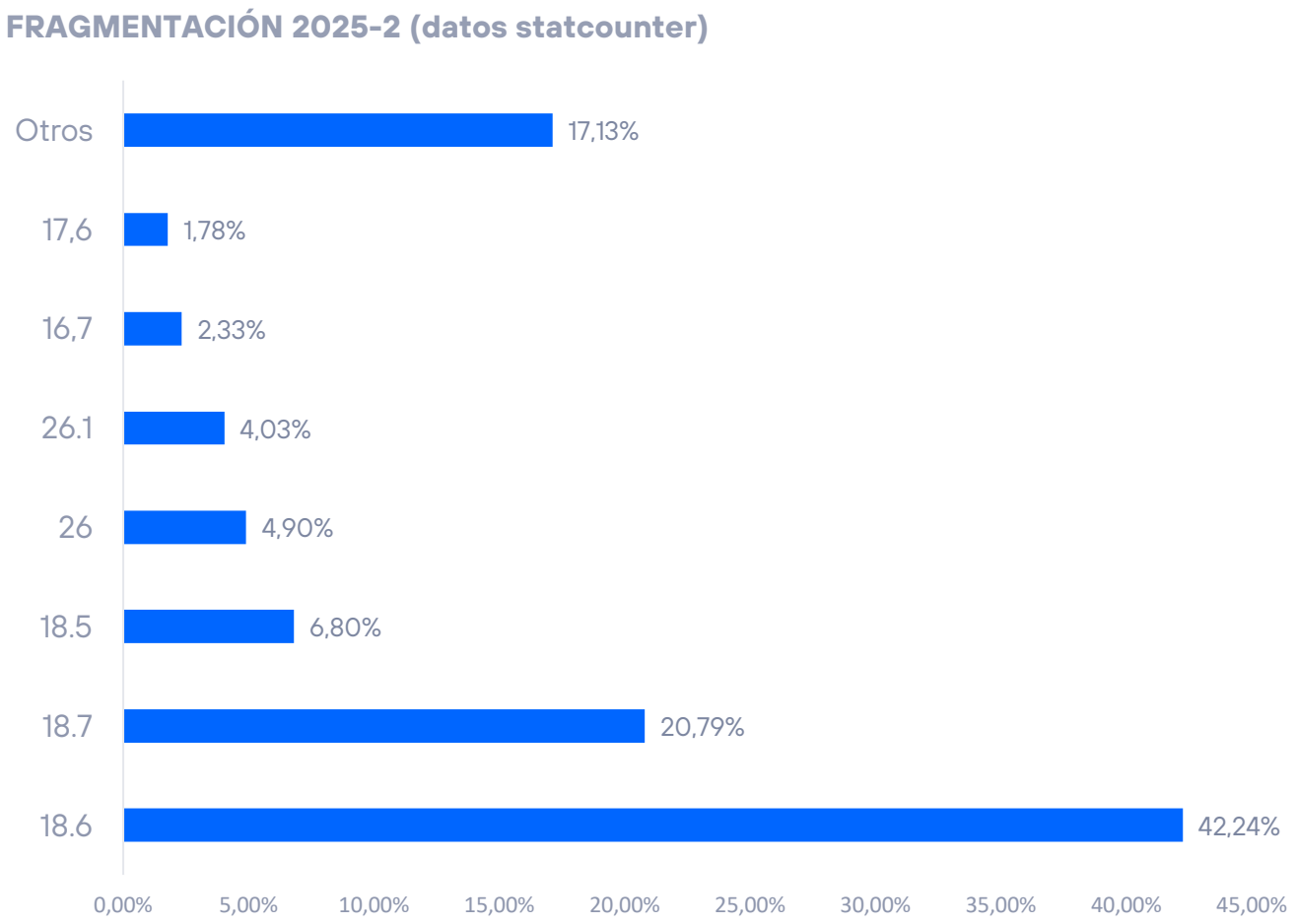
Entre todos ellos, multitud de fallos respecto de la privacidad, fallos en la gestión de memoria que podrían dar lugar a ejecución de código, etc.

Cerramos diciembre con iOS 18.7.3 con 21 parches y una nueva gran iteración para iOS 26, la 26.2 con precisamente 26 parches de diversa consideración.

Fragmentación de versiones durante el segundo 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.

Los tres primeros puestos del share son ocupados por iOS 18 y sus diferentes versiones. Es lógico, puesto que aún es una versión madura, extendida y la salida de iOS 26 es incipiente.



Tenemos un 17,13% de cuota que no especifica versión, con lo cual es un saco de versiones que no podemos identificar y podrían estar soportadas o no.

iOS 26 suma un cercano al 10%, dado que los datos son de noviembre, habrá que esperar al siguiente semestre para ver el impacto real a final de año.

La última versión con soporte de Apple es la iOS 18, estrenada en septiembre de 2024. El pasado semestre caducó el soporte para 16 y 15.

Android

Android 16 se consolida

Hasta el próximo año no tendremos una nueva versión de Android, que previsiblemente será la 17, pero no la veremos hasta casi la mitad de 2026 si se sigue cumpliendo el ritmo de estrenos del sistema operativo móvil de Google.

Vulnerabilidades

Android publica un conjunto de parches cada mes, generalmente durante la primera semana. En este segundo semestre de 2025 se han publicado seis boletines con la siguiente distribución de vulnerabilidades por cada mes:

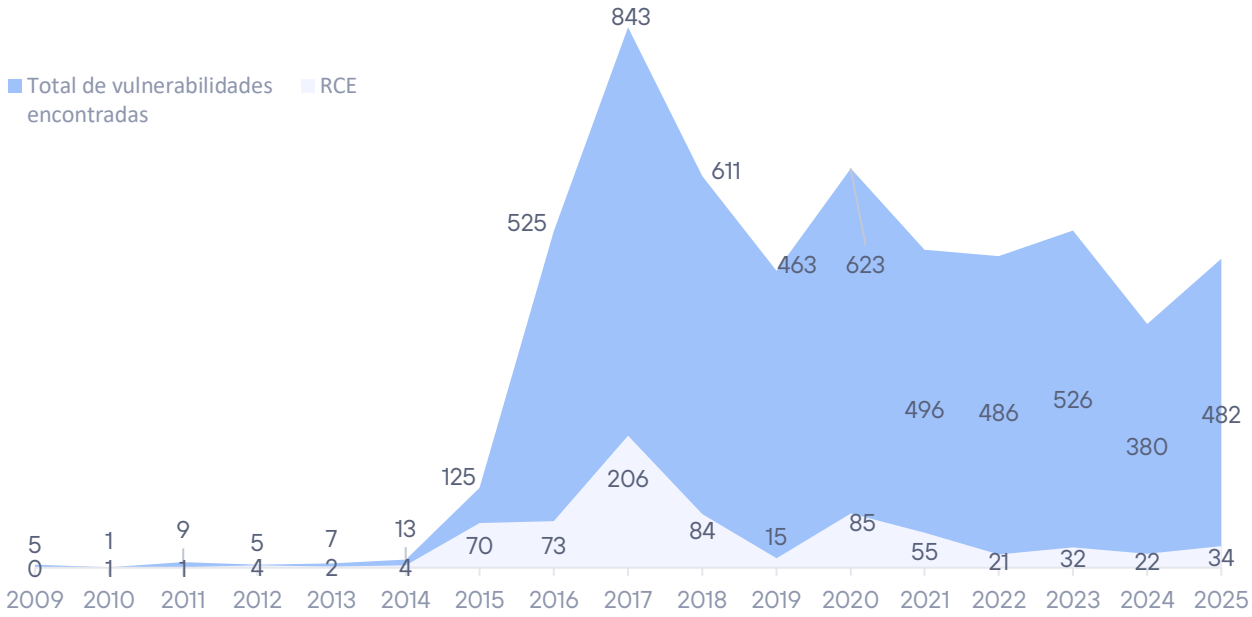
Mes	CVEs	Críticos o RCE
Julio	0	0
Agosto	6	1
Septiembre	110	3
Octubre	0	0
Noviembre	2	1
Diciembre	106	7

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, 224 parches en este semestre (el semestre anterior fue de 253); 12 de ellos considerados críticos (22 en el semestre anterior). El total en 2025 han sido 482 parches, 34 críticos.

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:
Evolución de vulnerabilidades por año



Fragmentación en sistemas Android

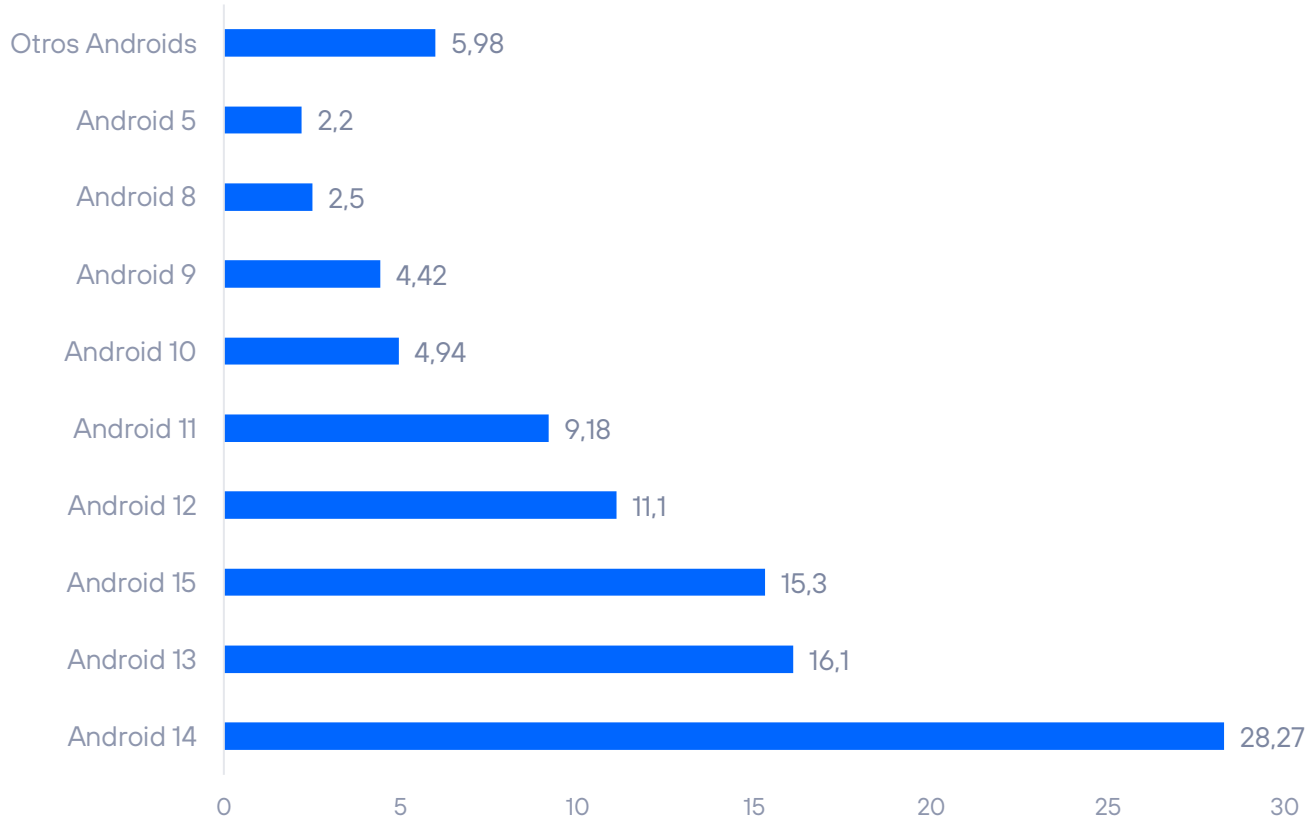
La última publicación de Statcounter a fecha de edición de este informe nos indican que la versión más implantada de Android es la 15, con un share de 28,27%. A pesar de la salida de Android 16 en junio del 2025 y como viene siendo habitual, las nuevas versiones de Android tardan en calar y acumular base de usuarios.

El ranking sigue habituándonos a ver un share preocupante de versiones de Android sin soporte.
Es decir, no reciben actualizaciones un casi 35% del parque de sistemas Android.

El pasado marzo finalizó el soporte de Android 12, por lo que solo las versiones superiores a esta reciben actualizaciones, cumpliéndose el plazo de 3 años de soporte desde el estreno del sistema operativo.

El ranking está en:

FRAGMENTACIÓN 2025-2



Podríamos preguntarnos con legitimidad ¿Qué hacen esas versiones tan antiguas de Android aún 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.

VULNERABILIDADES DESTACABLES

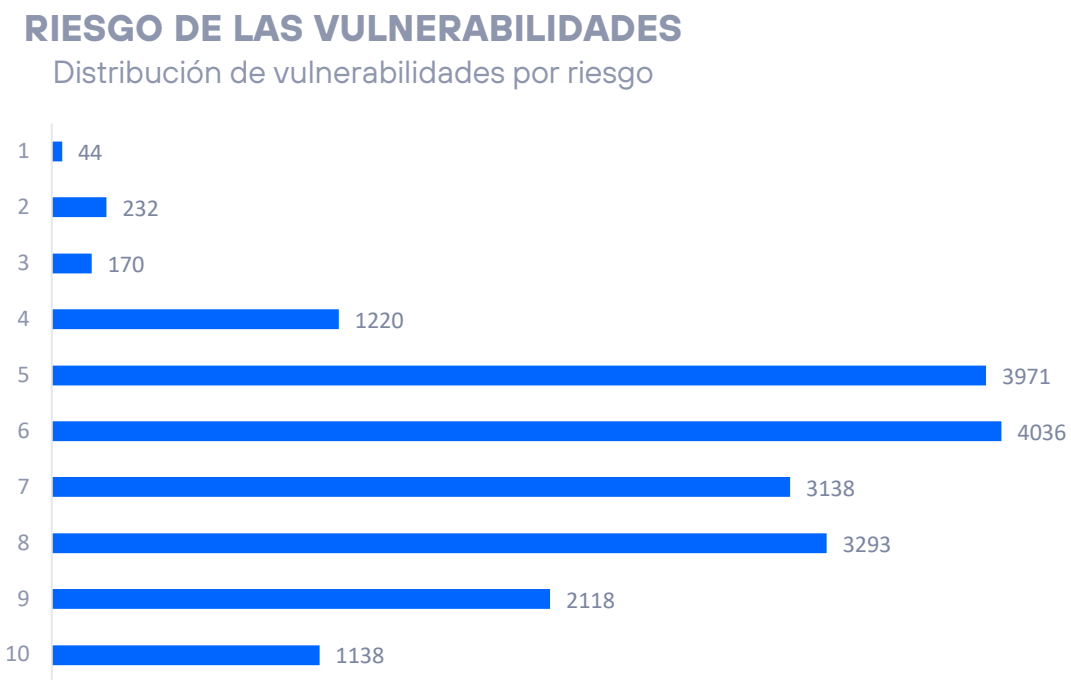
Comentamos en esta sección algunas de las vulnerabilidades notables a nuestro juicio, del segundo semestre de 2025.

CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2025-55182	React Server Components (React2Shell)	Permite control total del software a través de HTTP, fácilmente explotable de forma remota.	10
CVE-2025-8284	Packet Power Monitoring	La interfaz web de monitorización y control de potencia de paquetes no implementa mecanismos de autenticación. Esta vulnerabilidad podría permitir que usuarios no autorizados accedan y manipulen las funciones de monitoreo y control.	9.3
CVE-2025-9696	PVS6 de SunPower	Vulnerabilidad que podría permitir a los atacantes obtener acceso completo al dispositivo, lo que les permitiría reemplazar el firmware, modificar configuraciones, deshabilitar el dispositivo, crear túneles SSH y manipular los dispositivos conectados.	9.4
CVE-2025-10659	Telenium Online Web Application de Megasys Enterprises	Vulnerabilidad cuya explotación podría permitir a un atacante, no autenticado, inyectar comandos arbitrarios del sistema operativo a través de una solicitud HTTP diseñada, lo que daría lugar a la ejecución remota de código en el servidor en el contexto de	9.3
CVE-2025-12108	License Plate Recognition (LPR) Camera de Survision	No se requiere protección mediante una contraseña por defecto, lo cual posibilita el acceso inmediato al asistente de configuración sin tener que iniciar sesión o requerir de una verificación de credenciales.	9.3
CVE-2025-13510	Productos iHUB e iHUB Lite de Iskra	Falta de autenticación en los productos iHUB e iHUB Lite existente en la interfaz de administración web. Esto permite que usuarios no autenticados puedan acceder y modificar configuraciones críticas de los dispositivos.	9.3
CVE-2025-10035	License Servlet of Fortra's GoAnywhere MFT	Vulnerabilidad en el servlet que podría permitir a un actor con una firma de respuesta de licencia falsificada deserializar un objeto arbitrario, lo que llevaría a la inyección de comandos. En caso de que los archivos de	9.8

		registro contengan 'SignedObject.getObject' es probable que la instancia se haya visto afectada por esta vulnerabilidad.	
CVE-2025-6218	RARLAB WinRAR	Esta vulnerabilidad permite a atacantes remotos ejecutar código arbitrario. Para explotar esta vulnerabilidad, se requiere la interacción del usuario, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso. El fallo se encuentra en la gestión de rutas de archivo dentro de los archivos comprimidos. Una ruta de archivo manipulada puede provocar que el proceso acceda a directorios no deseados. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código	7.8
CVE-2025-8088	WinRAR	Una vulnerabilidad de recorrido de ruta que afecta a la versión de Windows de WinRAR permite a los atacantes ejecutar código arbitrario mediante la creación de archivos maliciosos.	8.4

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.



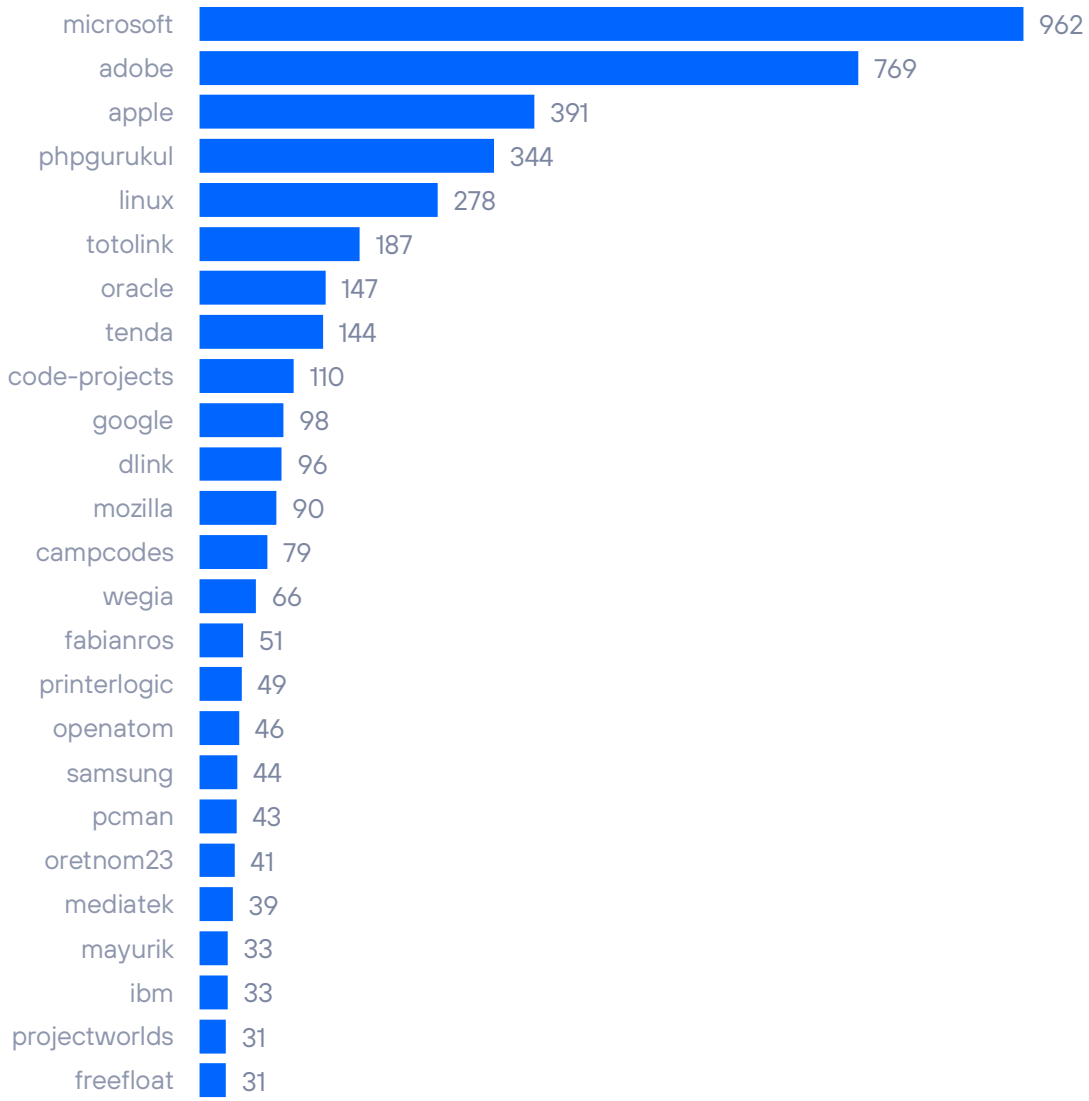
Top 25 compañías con más CVE acumulados

Este segundo semestre de 2025, Microsoft ha liderado con cierta diferencia por número de vulnerabilidades conocidas, seguido de Linux y Apple. Ya va siendo habitual verlos en las tres primeras posiciones.

El resto de los fabricantes lo componen tanto grandes organizaciones como desarrolladoras de software de tamaño mediano e incluso pequeñas firmas.

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 segundo semestre de 2025

APT36 – Transparent Tribe: Un leopardo difícil de detectar

12 años encargándose de operar siguiendo los intereses de Pakistán, concretamente orientándose a India. Recientemente, siguiendo esta planificación, se detectó una campaña de ciber espionaje dirigida contra instituciones gubernamentales indias.

La campaña está dirigida contra sistemas Linux Boss (Bharat Operating System Solutions) una distribución india basada en Debian. Su vector de entrada es un e-mail de phishing (información en PDF) con un enlace a un ZIP (o directamente el ZIP) situado en un servicio como Google Drive o un servidor dedicado de staging. El ZIP ejecuta el RAT DeskRAT.

También a lo largo de este semestre, aunque sean campañas distintas, este actor lanzó otro phishing en el que, con la excusa de una reunión, solicitaba información a su víctima. Entre otra información, se solicitaba el código de Kavach. Kavach es una aplicación 2FA desarrollada por el Centro Nacional de Informática (NIC) para mejorar la seguridad de los servicios de correo electrónico del gobierno en India, generando OTP basados en tiempo. Junto con la contraseña del usuario y la dirección de e-mail, los atacantes ya tenían lo necesario para autenticarse en los sistemas del gobierno indio.

Más información en https://blog.sekoia.io/transparenttribe-targets-indian-military-organisations-with-deskrat/

Lazarus: Se levanta, anda... y triunfa

Lazarus vuelve a la palestra por segundo semestre consecutivo.

En este caso, fueron descubiertos dirigiendo su actividad contra empresas europeas de defensa involucradas en el desarrollo de drones: una metalúrgica, un fabricante de componentes aeronáuticos y un contratista de defensa. Los investigadores de ESET engloban esta actividad en una campaña denominada Dream Job, en la que participan varios grupos de varios países.

La manera de comprometer la seguridad de sus objetivos era la siguiente: Ingeniería social (ofertas de trabajo) en formato PDF que forzaba la apertura de un lector "troyanizado". A partir de ahí, se instala el RAT ScoringMathTea, detectado por primera vez en 2022 en campañas en Portugal y se toma el control de los sistemas para recopilar información sobre estos sistemas.

Más información en: https://www.eset.com/us/about/newsroom/research/north-korean-lazarus-group-targets-drone-sector-europe/

Primitive Bear: sigue evolucionando

Otro actor que hace doblete en nuestro informe en 2025. En este caso ha sido detectado participando en acciones de espionaje contra Ucrania. Sus labores se han centrado en la extracción de inteligencia de alto nivel del gobierno ucraniano.

Para seguir viviendo, el oso sigue evolucionando. En esta campaña empleó una técnica de camuflaje de dominios de la lista blanca para construir URL maliciosas. Este método utiliza una sintaxis legítima (usuario:contraseña@host). A partir de ahí, emplean infraestructura del Servicio de Tunelización para Desarrolladores de Microsoft para obtener un certificado TLS válido (emitido por MS) y ocultar su actividad entre el flujo legítimo.

Más información en: https://cn-sec.com/archives/4411359.html

Volt/Salt Typhoon: Dos tifones rodean Australia

El jefe de inteligencia australiano, Mike Burgess, afirmó que al menos dos grupos patrocinados por el Estado chino se están posicionando para futuras operaciones de sabotaje y espionaje contra redes australianas, lo que genera serias preocupaciones de seguridad nacional sobre la intrusión cibernética preventiva y la posible interrupción de infraestructuras críticas.

Según Burgess, el grupo Volt Typhoon estaría apuntando a redes eléctricas, de agua y transporte, mientras que Salt Typhoon se estaría centrando en las redes de telecomunicaciones australianas.

Estos grupos no son nuevos y de hecho, ya habrían sido reconocidos según medios de comunicación, como el Wall Street Journal, como parte de acciones de represalia contra Estados Unidos por su apoyo a Taiwán.

Más información en: https://securityaffairs.com/184540/intelligence/australias-spy-chief-warns-of-china-linked-threats-to-critical-infrastructure.html

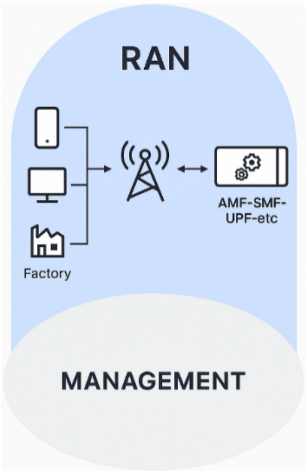
ANÁLISIS DE AMENAZAS OT

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.

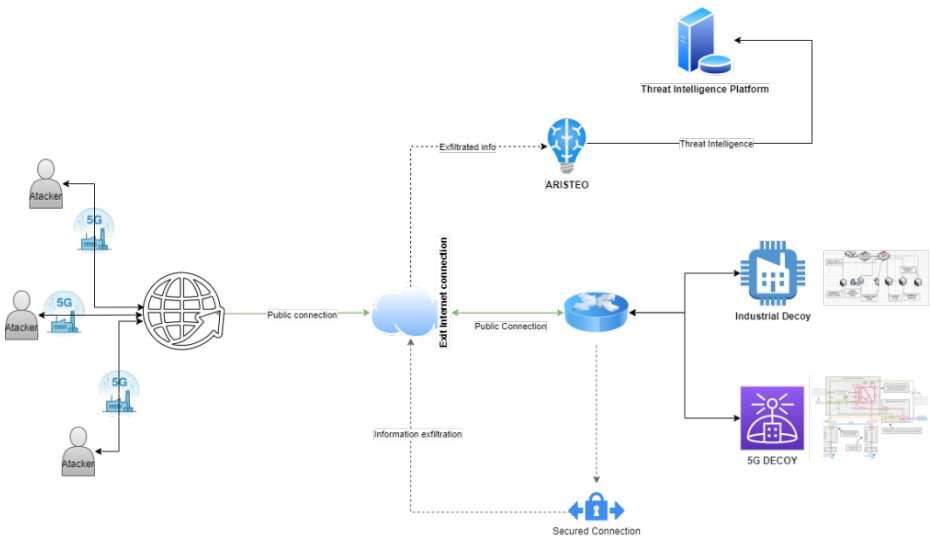
Análisis de la información

Este semestre tenemos nuevas noticias para Aristeo. A sus capacidades naturales para extraer información de dispositivos y redes industriales (a través de su red de señuelos), se une la capacidad para extraer información de señuelos 5G. Conocedores de que las redes 5G privadas son cada vez más usadas en entornos industriales, pensamos que era el momento de dar un paso más con Aristeo e introducir este concepto en su red de señuelos.



El señuelo podría recibir interacción de atacantes desde el entorno de administración (a través de un acceso remoto) y desde el espectro radioeléctrico. Sin embargo, para emplear este último vector de ataque, el atacante debería estar dentro del radio de la antena. En entornos en los que el cliente no busque monitorizar sus alrededores (un entorno operativo típico), el señuelo emula tráfico de dispositivos en la red 5G.

Por supuesto, siguiendo la misión de evitar elementos superfluos en la red de señuelos y darle una apariencia de legitimidad, el sistema está integrado de la siguiente forma:



Como se puede observar, el señuelo 5G se encuentra dentro de la infraestructura de un señuelo industrial. De esta forma, da la apariencia de ser un entorno privado para el despliegue de una burbuja 5G en dicho entorno industrial. Además, un atacante aún podría intentar acceder haciendo un movimiento lateral a través del compromiso de alguno de los dispositivos del señuelo industrial. Como el sistema es operable, el atacante puede dar de alta dispositivos, alterar configuraciones, recoger tráfico entre los dispositivos y la antena (sea esta física o virtual, como indicábamos antes) o intentar manipular los valores de los dispositivos industriales dentro de la misma red.

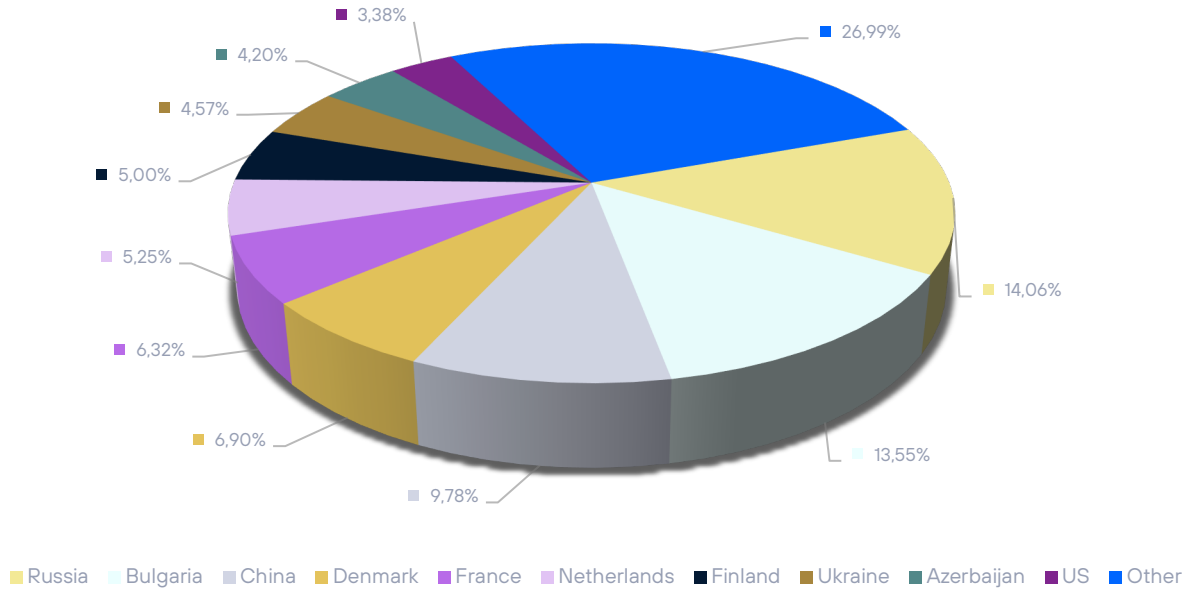
Pasamos a la estadística general de la información registrada. En el segundo semestre de 2025 se detectaron 43 millones de eventos de ciberseguridad. Llegados a este punto y por última vez (que ya lo hemos dicho varias veces), conviene recordar que se trata de eventos complejos, y que, gracias a Aristeo 2.0, los eventos ahora se asocian entre sí, lo que convierte los más de 214 millones de eventos "simples" que hemos tenido este semestre en esa cifra de 43. Esta cifra supone una caída acusada de la actividad respecto al semestre pasado y al mismo periodo (segundo semestre) de 2024.

La razón para este descenso, al menos en parte, tiene que ver seguramente con el ataque dirigido por parte de un actor profesional a uno de nuestros señuelos permanentemente conectados a estas estadísticas. Dimos más detalles de este ataque dirigido en el informe semestral anterior y en una entrada en el blog de Telefónica Tech, pero su actividad se extendió hasta julio de 2025. Esto nos llevó pausar la actividad de este señuelo mientras implementábamos lo aprendido de este actor tras un profundo análisis forense.

Centrándonos, ahora sí en los análisis estadísticos propios de este informe, la distribución por países sería la siguiente:

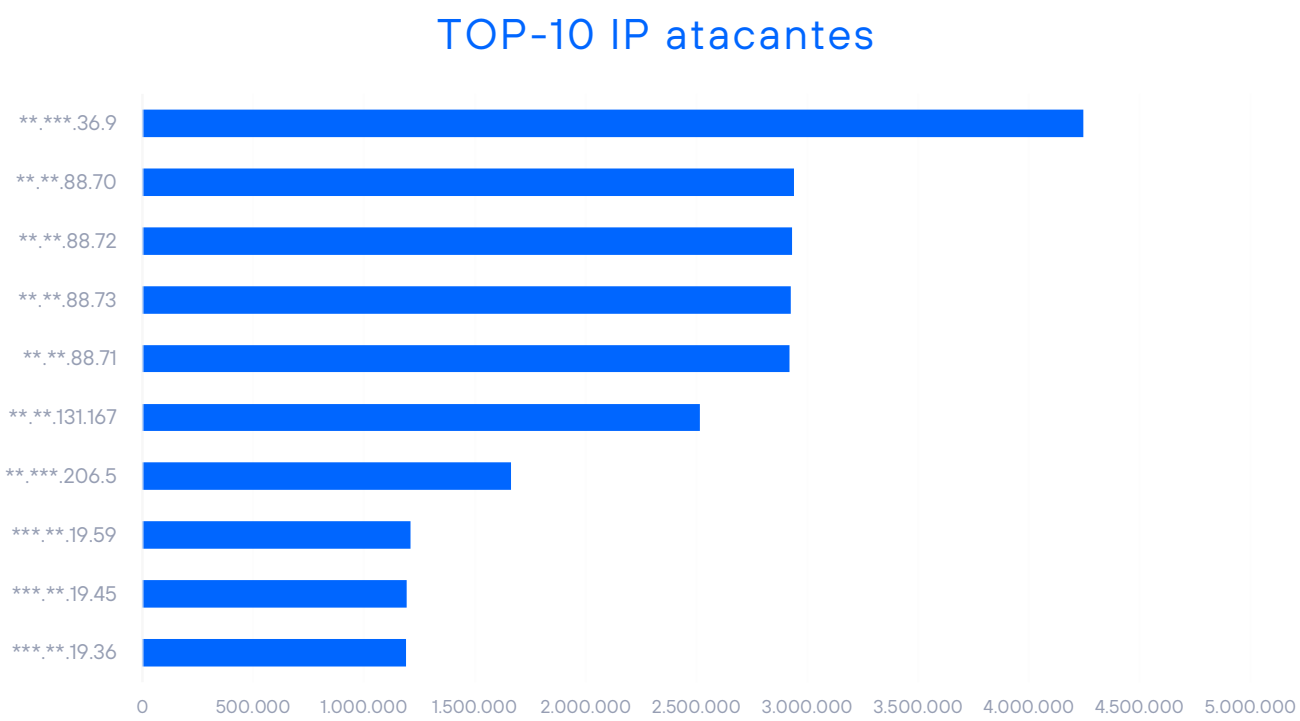
La distribución por países sería la siguiente:

Interacciones - 2025H2

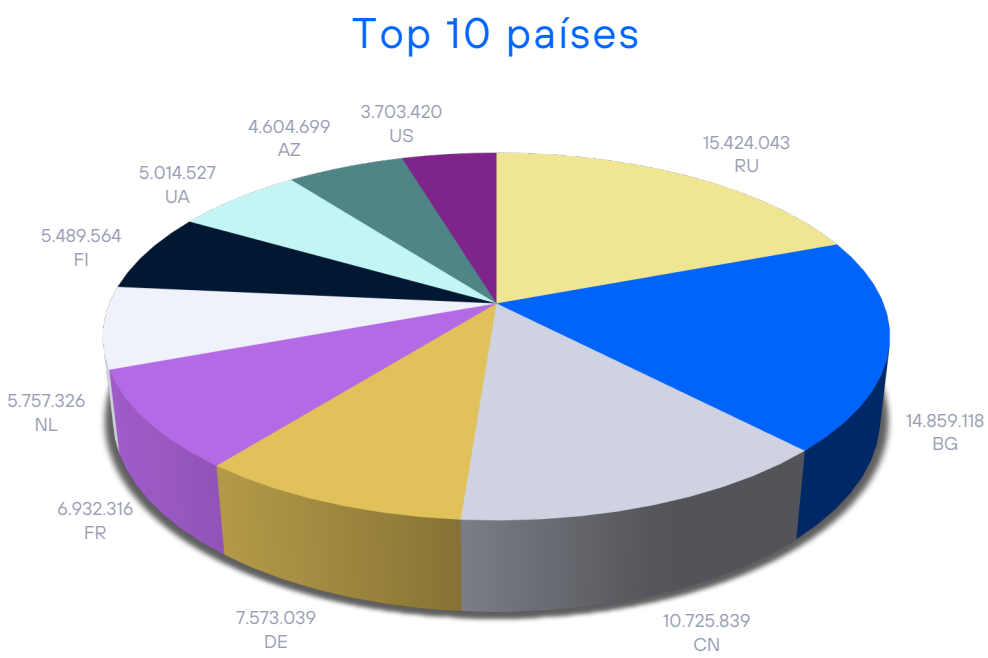


Este semestre, el top-10 lo encabeza Rusia, mientras que Bulgaria, país ganador el semestre pasado, baja la segunda posición. La dispersión ha cambiado respecto al semestre pasado, donde el primer clasificado aglutinaba un 36% de los eventos y los demás se volvían menos representativos. Este semestre no se da esa situación.

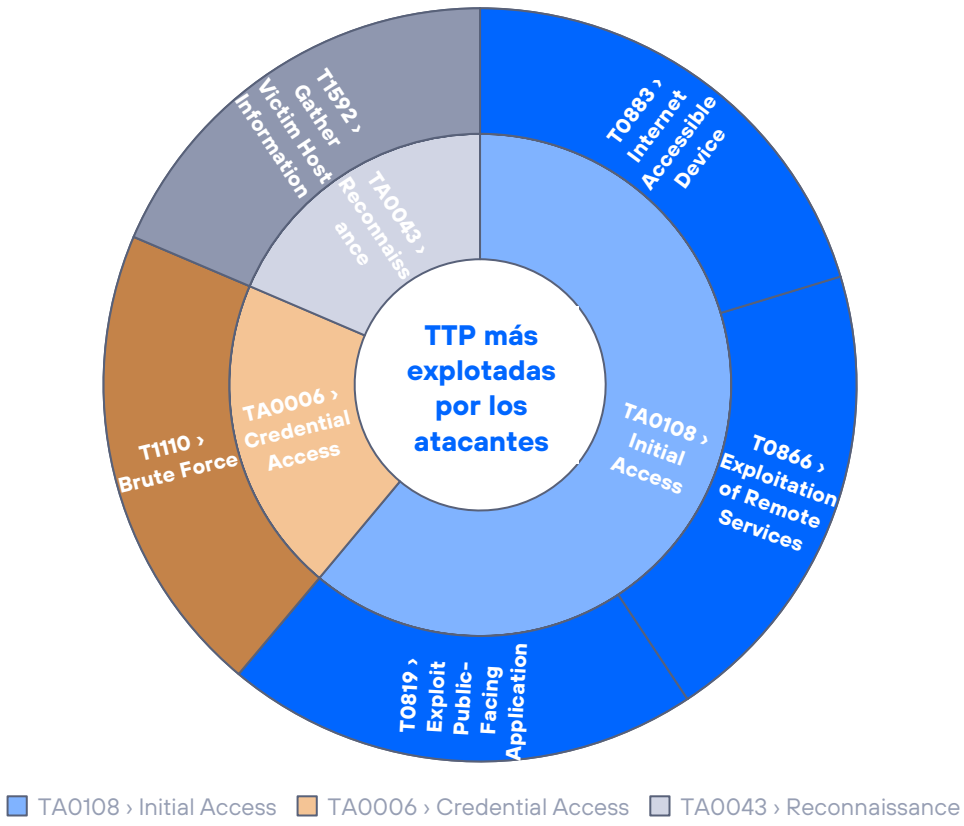
Ahora vamos a ver las diez direcciones IP con más interacción con el sistema de Aristeo. En este semestre, los países con más visitas a Aristeo son los que posicionan mayoritariamente sus IP en la lista. En este caso, se podría hablar de cierta estabilidad. Sin embargo, también podríamos decir que el TOP 10 (nosotros vemos las IP sin ofuscar) está conformado por bloques de direcciones IP y su actividad está relacionada con más acciones automatizadas y coordinadas de aproximación y descubrimiento. Parece que vuelve el ciclo de búsqueda y revisión de la seguridad de los dispositivos que flotan por internet.



A continuación, vemos cómo se reparten el *top 10* de los países registrados. Como comentamos anteriormente, las interacciones en Aristeo han estado más repartidas que el semestre anterior. A ello ha contribuido el aumento de actividad desde Rusia y China, dos países que el semestre pasado tuvieron una actuación muy discreta.



Este semestre, gracias a Aristeo 2.0, volvemos a ejecutar el análisis de las TTP (Tácticas, Técnicas y Procedimientos) más explotadas por los atacantes, pero con un gráfico distinto del semestre anterior.



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 o los ataques dirigidos a servicios y dispositivos accesibles. Otras acciones fuera del TOP 5, como 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: 334.335 direcciones IP, 228.954 dominios y 486.004 URLs.

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:

Phishing	212.556	43,74%
Malware Download	95.334	19,62%
Whatsapp Phishing	20.885	4,30%
Naver Phishing	19.251	3,96%
Trojan.generic	18.427	3,79%
Trojan.phishing.pdf	17.246	3,55%

Booking Phishing	6.590	1,36%
Malicious.PDF	6.001	1,23%
Facebook phishing	4.675	0,96%
Rakuten phishing	4.641	0,95%

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.

A destacar la presencia de nuevos tipos de amenaza de los que ya teníamos noticia: los phishings especializados en marcas concretas: Facebook, Rakuten, Booking, etc. Son de largo los que más acumulan positivos. La estrategia es clara: hacerse pasar por estas marcas conocidas y que transmiten confianza para hacer bajar la guardia de la posible víctima.

El resto se reparte, como vemos, por categorías genéricas, que incluyen todo tipo de vectores y amenazas: malware inserto en documentos o troyanos de diverso tipo.

¿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 el que nos "chivará" dónde se ha alojado y de qué servicio ha hecho uso (ilegítimo).

ru.com	21.067	4,33%
google.com	9.881	2,03%
pages.dev	7.618	1,57%
vercel.app	6.847	1,41%

za.com	6.836	1,41%
sa.com	5.902	1,21%
checkin-arrivals.com	5.823	1,20%
weebly.com	4.873	1,00%
github.io	4.494	0,92%
duckdns.org	2.563	0,53%

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.

Estados Unidos	67.172	20,09%
China	31.376	9,38%
India	24.325	7,28%

Brasil	14.227	4,26%
Países Bajos	12.312	3,68%
Vietnam	12.115	3,62%
Alemania	11.478	3,43%
Rusia	10.730	3,21%
Singapur	10.199	3,05%
Canadá	9.879	2,95%

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?

Suspicious host	157.456	47,10%
Malicious host	156.157	46,71%
HTTP Spammer	97.928	29,29%
Mail Spammer	86.382	25,84%
SSH Attacker	46.492	13,91%
Bruteforce	40.668	12,16%
DDoS Attacker	37.612	11,25%
HTTP Attacker	36.094	10,80%

Port Scanner	35.594	10,65%
Hacking	34.796	10,41%

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 13,91% 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 12,16%, algo menos respecto a la anterior cifra.

En otra subcategoría (10,65%), escaneos indiscriminados, encontramos: Port 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.

De forma general, encontramos la categoría "hacking" con un 10,41% 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:

com	71.573	31,26%
top	25.381	11,09%
shop	19.612	8,57%
ru	14.465	6,32%
app	8.268	3,61%
dev	7.534	3,29%
click	7.419	3,24%
xyz	6.721	2,94%
org	5.453	2,38%
cn	5.108	2,23%

"com" vuelve a coronar en este semestre nuestro ranking de TLDs destronando a "xyz", sin duda empujado por ese "ru.com" que comentábamos anteriormente. Además lo hace con fuerza, casi triplicando las cifras del perseguidor.

"shop" sube con fuerza. El TLD especializado en e-commerce es objetivo común en phishings que se hace pasar precisamente por marcas de venta online, da confianza a las víctimas y no muchos dominios poseen alta en este TLD; que además es bastante económico.

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.

El resto de dominios lo componen los sospechosos habituales que siempre entran en el ranking.

¿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	149.014	65,08%
ClearFake	141.800	6,19%
Generic Malware	9.394	4,10%
Malware Download	7.590	3,32%
MetaStealer	5.039	2,20%
Necurs	4.015	1,75%
WhatsApp Phishing	3.866	1,69%
Command and Control	3.560	1,55%
Orchard	3.090	1,35%
Phishing Allegro	2.488	1,09%

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

Cómo hacer frente a los fraudes telefónicos: así se intentan proteger España y otros países de Europa contra este tipo de estafas

Ciberinteligencia en OT: anticiparse al ataque

Del papel a la acción: cómo construir una hoja de ruta de ciberseguridad OT eficaz

INTELIGENCIA ARTIFICIAL

Sandbox de IA: entornos seguros para la evaluación y protección de modelos de Inteligencia Artificial

Quantum Machine Learning: ¿la próxima revolución en la IA?

¿Confías en esa IA? Las credenciales verificables son tu garantía