Telefónica Tech

Informe sobre el estado de la seguridad 2024 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

Índex

RESUMEN EJECUTIVO

El objetivo de este informe es sintetizar la información sobre ciberseguridad de los últimos meses (desde la seguridad en móviles hasta las noticias más relevantes y las vulnerabilidades más habituales), adoptando un punto de vista que abarque la mayoría de los aspectos de esta disciplina, para así ayudar al lector a comprender los riesgos del panorama actual.

Durante el segundo semestre de 2024 han destacado principalmente dos noticias. El 19 de julio se produjo un parón tecnológico a nivel mundial. Alrededor de 8.5 millones de sistemas Windows comenzaron a reiniciarse con pantallas azules, una y otra vez, sin remedio remoto para solucionarlos. Los titulares se adelantaron: un fallo en Microsoft. Pero poco después, CrowdStrike admitía que su producto Falcon había sufrido una actualización defectuosa que, al ejecutarse en el kernel, provocaba este grave error.

Este incidente iba más allá del problema puntual ocurrido ese día. Planteaba serias dudas sobre la responsabilidad de un proveedor de ciberseguridad en Windows. ¿Cómo podía un error en un solo producto paralizar a medio mundo? ¿Hasta dónde llegaba la responsabilidad de Windows al permitir ejecutar contenido no validado en el entorno del kernel? Poco después del incidente, comenzaron las acusaciones e incluso las demandas por pérdidas.

Y como consecuencia, lo positivo es que la propia Microsoft se plantea reestructurar su propio sistema de integración con los EDR, para que esto no pueda ocurrir. Porque la dicotomía está servida: Crowdstrike quería actualizar rápido para proteger más, pero rápido y bien, suelen ser características contrapuestas.

Veremos consecuencias directas de este problema en los años venideros, tanto en el diseño del propio Windows como en el de los EDR.

Por otro lado, Ivanti, Cisco, Fortinet, PaloAlto... empresas que protegen los perímetros de millones de empresas, han vuelto a sufrir gravísimas vulnerabilidades, mucho más frecuentemente de lo deseado. En concreto, Ivanti ha sufrido una serie de 0days desastrosos durante todo el segundo semestre del año, la mayoría de ellos encontrados, (como indica el propio término 0day) mientras los atacantes los aprovechan.

Estas dos observaciones destacadas durante el semestre nos deben hacer reflexionar sobre los problemas derivados de los propios sistemas de protección, que merecen una atención especial. No se va a poder evitar que sean vulnerados, pero al menos sí que es posible una gestión más segura que permita un bastionado previo y una respuesta rápida si se consuma un incidente.

Al final, todo depende de la eterna pregunta: ¿Quién vigila al vigilante?

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 2024

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

JULIO

- **CrowdStrike Falcon EDR**: Una actualización defectuosa de CrowdStrike afectó a más de 8 millones de sistemas Windows. El incidente causó bastante revuelo tanto en la operativa mundial como en la información otorgada por todo tipo de medios. Desde un ataque global hasta un fallo en la propia Microsoft (dado que se manifestaba con la famosa pantalla azul).
  CrowdStrike Falcon es un EDR centrado en empresas, así que el incidente provocó la caída de sistemas de TI cruciales a nivel global.
- **Importante vulnerabilidad en un plugin de WordPress**: El equipo de WPScan descubrió una vulnerabilidad importante en un **plugin popular de WordPress llamado Profile Builder** y su versión comercial, Profile Builder Pro. La vulnerabilidad **permitía a los actores malintencionados obtener acceso de administrador sin tener ningún tipo de cuenta en el sitio**.
- Grupo de fraude telefónico detenido: Las **fuerzas de seguridad españolas y portuguesas arrestaron a 54 individuos sospechosos de robar 2,5 millones de euros a personas mayores utilizando estafas telefónicas**. El grupo operaba contactando a las víctimas por teléfono y haciéndose pasar por empleados de bancos. Convencían a los usuarios para que revelaran credenciales bancarias o entregaran sus ahorros a un mensajero que se presentaba en su puerta. El dinero robado luego se blanqueaba a través de la red de cuentas bancarias del grupo.
- **Vulnerabilidad ServiceNow**: CISA y varias empresas de seguridad advirtieron que dos vulnerabilidades de ServiceNow que fueron reportadas por AssetNote el 11 de julio están siendo explotadas activamente, entre ellas, la vulnerabilidad crítica CVE-2024-4879. **Estas vulnerabilidades permiten a los atacantes acceder a bases de datos y exfiltrar datos, así como leer archivos arbitrarios**. Los investigadores advierten de entre 13 mil y 42 mil instancias vulnerables de ServiceNow que abarcan tanto sectores privados como públicos.
- **Cuello de botella en el procesamiento y enriquecimiento de vulnerabilidades del NIST**. La Base de Datos Nacional de Vulnerabilidades (**NVD**) lleva acumulando un importante retraso desde febrero y, aunque en mayo se anunció la contratación de un nuevo proveedor, el *backlog* no ha dejado de crecer situándose en más de **17000 vulnerabilidades sin procesar**. Esto supone un **impacto en la gestión de vulnerabilidades de la comunidad de ciberseguridad global**, que depende en gran medida, de esta información **para ayudar a informar a los clientes sobre qué errores corregir primero**.
- **La agencias de ciberseguridad estadounidense, CISA, publicó un aviso en el que se detalla,** entre otras, un conjunto de explotaciones del controlador industrial de Honeywell ControlEdge Virtual UOC. Este sistema es una máquina virtual basada en Linux que elimina la necesidad de un controlador físico. Un atacante podría tomar el control total del controlador y un acceso a toda la red OT donde éste se encuentre.

AGOSTO

- *Exploit* para vulnerabilidad RCE en Windows: Este mes se publicó un código de prueba de concepto (PoC) en GitHub para **la vulnerabilidad de ejecución remota de código en la pila TCP/IP de Windows**, **afectando a sistemas con IPv6 activado**. Identificada como **CVE-2024-38063** y con un **CVSSv3 de 9.8** según Microsoft, **permitía a atacantes explotar sistemas Windows 10, 11 y Server sin necesidad de interacción del usuario, mediante el envío de paquetes IPv6 especialmente diseñados** que desencadenan un desbordamiento de búfer.
- **Generación de QRs con Unicode**: Atacantes cran un innovador método para crear QRs con caracteres Unicode y así engañar a los sistemas de protección de correo electrónico. Los caracteres Unicode permiten secuenciar caracteres de "bloques" de color negro sobre blanco y diferente tamaño que, perfectamente alineados, formarán un QR perfectamente identificable por cualquier cámara. **Sin embargo, para el sistema de análisis de correo, ya no será ni una URL, ni una imagen, sino texto de nuevo, y le resultará, por ahora, imposible deducir que en esa combinación de "bloques" se oculta un código QR**.
- **Digicert** se ve obligado por un lado a revocar en horas más de 83.000 certificados de casi 7.000 clientes por un fallo de comprobación de seguridad. Pero por otro**, ha tenido que posponer la revocación y ampliar el plazo para aceptar excepciones en infraestructuras críticas**.
- Ataque *Sinkclose* de AMD: Investigadores de seguridad descubren un fallo de seguridad en los procesadores AMD, denominado Sinkclose, con identificador CVE-2023-31315. Esta vulnerabilidad afecta a casi toda la línea de CPUs de AMD desde 2006. La vulnerabilidad permite a los atacantes ejecutar código malicioso en el Modo de Gestión del Sistema privilegiado del chip.
  Aunque se requiere un acceso inicial, *Sinkclose* permite la instalación de *malware* profundamente arraigado que puede sobrevivir a la reinstalación del sistema operativo y ser extremadamente difícil de eliminar.
- **Pavel Durov, CEO y fundador de Telegram detenido en Francia**: Las autoridades francesas detienen al CEO y fundador de Telegram. Durov fue detenido en una **investigación relacionada con la falta de moderación de contenido en Telegram**. El popular servicio de mensajería instantánea está siendo utilizado, de forma cada vez más frecuente, para la actividad criminal: datos personales robados, tarjetas robadas, *malware* y otros tipos de contenido ilegal.
- Investigadores de la universidad de California han descubierto una vulnerabilidad en el cambio de marchas wireless para bicicletas de Shimano. La explotación de la vulnerabilidad no es compleja y puede realizarse a una distancia de hasta 9 metros. El atacante toma el control total del cambio: puede cambiar de marchas o bloquear el cambio en una marcha concreta.

SEPTIEMBRE

- **Explosiones de buscas en el Líbano**: Miles de personas resultaron heridas después de que buscapersonas, supuestamente utilizados por miembros de Hezbollah, explotaran. Informes posteriores parecen indicar que este no fue el caso y que la realidad fue que se interceptó un envío de buscapersonas y se añadieron cargas explosivas que podían ser detonadas de forma remota.
- **Fuga de datos de MC2**: El servicio de verificación de antecedentes MC2 Data dejó **expuesto** un servidor de base de datos que contiene los datos personales de más de **100 millones de ciudadanos estadounidenses**. CyberNews informa que la base de datos, de 2.2TB, contiene

información extremadamente sensible, que va desde **nombres hasta registros de propiedades, detalles de empleo y documentos legales**.

- Coches Kia comprometidos: Un equipo de investigadores de seguridad encuentrauna **vulnerabilidad en el portal web de Kia que les permitió tomar el control de millones de coches de la compañía**. Los investigadores construyeron una herramienta personalizada que les daba control sobre funciones clave del coche. Esto incluía la **capacidad de desbloquear puertas, hacer sonar la bocina o arrancar el motor**. El equipo de investigación notificó a Kia sobre el fallo en junio, y la compañía parcheó su portal web en agosto.
- Vulnerabilidad crítica de Linux en el Common UNIX Printing System (CUPS): esta vulnerabilidad permitía a los atacantes ejecutar comandos en un ordenador objetivo a través de trabajos de impresión maliciosos. La vulnerabilidad requiere condiciones específicas para ser explotada. A su vez Akamai ha descubierto que el sistema CUPS puede ser abusado para lanzar ataques DDoS a gran escala. Un atacante puede enviar un solo paquete a un servidor CUPS que lo amplificará y retransmitirá a un objetivo deseado.
- Kemp Technologies soluciona una vulnerabilidad importante en sus dispositivos de balanceo de carga *LoadMaster* que puede permitir a actores malintencionados ejecutar código malicioso en el dispositivo. Identificada como CVE-2024-7591, la vulnerabilidad es un error de validación de entrada en el panel de gestión del dispositivo y puede permitir a los actores malintencionados ejecutar comandos del sistema operativo. Kemp lanzó una actualización de seguridad la semana pasada y alentó a los clientes a actualizar antes de que la vulnerabilidad sea explotada en el entorno. **La vulnerabilidad recibió una puntuación de severidad de 10/10 debido a su facilidad de explotación.**
- **Australia introduce una ley contra el *doxxing***: El fiscal general de Australia presenta un proyecto de ley que prohibirá la publicación de información personal en línea, también conocida como *doxxing*. La ley propuesta enmienda la Ley de Privacidad de Australia de 1988 e impone una pena de prisión de hasta siete años para los infractores. También este gobierno planea introducir una novedosa legislación para introducir una edad mínima para el uso de redes sociales.
- La agencia de ciberseguridad estadounidense, CISA, ha vuelto a publicar un anuncio advirtiendo de la relativa facilidad con la que se pueden atacar con éxito los sistemas industriales, además de la sencillez de éstos. Este anuncio fue precedido por el ciberataque que recibió la planta de aguas de Arkansas City, de 12.000 habitantes. Dicha planta tuvo que volver a operaciones manuales tras perder el control de sus sistemas.

OCTUBRE

- Por supuesto que los atacantes usarán la IA para hacer más realistas sus ataques de ingeniería social. Pero también, de una forma mucho más simpe y barata, como reclamo de ingeniería social en sí misma. Eso ha pensado el grupo FIN7 que, tras muchos años preparando sofisticadas campañas, han encontrado una fórmula interesante para infectar a sus víctimas. Se ha hecho público que FIN7 está utilizando al menos siete sitios web que anuncian generadores de desnudos con IA como señuelo para engañar a las víctimas y hacer que se infecten con *malware*. Está ofreciendo una prueba gratuita del software generador de desnudos con IA que contiene una versión del NetSupport RAT.

- Se detecta una **vulnerabilidad que afecta a muchos miles de semáforos en Holanda y que obligará a la sustitución manual de los mismos como única posibilidad de remediación**, en un proyecto de alto coste, que el gobierno holandés ha estimado que se prolongará durante seis años hasta el año 2030.
- El Consejo de la UE aprobó el Acta de Resiliencia Cibernética. La nueva ley introduce requisitos mínimos de ciberseguridad para los productos digitales vendidos en la UE. Según las nuevas reglas, los proveedores deben proporcionar actualizaciones de seguridad gratuitas y automáticas, soportar los productos durante al menos cinco años y gestionar un programa de divulgación de vulnerabilidades. Las empresas también deben notificar a la agencia de ciberseguridad de la UE cuando se explote una vulnerabilidad en sus productos. **Los productos que cumplan con los requisitos mínimos de la CRA podrán colocar la marca CE en la etiqueta de su producto**.
- Nueva especificación para la **migración de *Passkeys***: La **FIDO Alliance** publica una nueva especificación para una nueva tecnología que permitirá a los usuarios mover fácilmente las claves de acceso entre plataformas y proveedores. Actualmente, cuando un usuario quiere transferir credenciales de un gestor de credenciales a otro, la transferencia generalmente se realiza de manera insegura y en claro.
- **Guía de malas prácticas de CISA**: En un giro poco común (habitualmente se destacan y recomiendan las buenas prácticas), CISA publica una "guía" con las malas prácticas más comunes en las que los proveedores de software aún están incurriendo, con la esperanza de que las empresas sientan la presión y comiencen a adoptar un enfoque de Seguridad por Diseño.
- Nuevo **récord de DDoS bloqueado por Cloudflare**: Durante una campaña de denegación de servicio distribuida dirigida a organizaciones en los sectores de servicios financieros, internet y telecomunicaciones, los ataques volumétricos alcanzaron un pico de 3.8 terabits por segundo, el más grande registrado públicamente hasta la fecha. El asalto consistió en una "embestida de un mes" de más de 100 ataques DDoS. **Cloudflare mitigó todos los ataques DDoS de forma autónoma y señaló que el que alcanzó un pico de 3.8 Tbps duró 65 segundos**.
- Un informe publicado por OpenAI revela que la compañía de inteligencia artificial ha interrumpido más de 20 operaciones cibernéticas desde principios de año, incluidas las actividades de APT-Group patrocinados por el estado iraní y chino. Los grupos fueron detectados en varios ataques a plantas de agua de Irlanta y EEUU.
  Según OpenAI, las cuentas asociadas utilizaron ChatGPT para realizar reconocimientos, pero también para ayudarlogoldens con la explotación de vulnerabilidades, la evasión de la detección y la actividad posterior al compromiso.

NOVIEMBRE

- **Google AI encuentra una vulnerabilidad en SQLite**: Google con su sistema de IA Big Sleep encuentra su primera vulnerabilidad válida en un proyecto del mundo real: el motor de base de datos SQLite. La vulnerabilidad fue descrita como un desbordamiento de búfer. El problema se encontró en una versión de desarrollo de la base de datos y se solucionó antes de que el código vulnerable se enviara a los consumidores.
- **Brecha de seguridad en Finastra**: Finastra, proveedor de 45 de los 50 bancos más grandes del mundo, reconoce un incidente. Un atacante ha accedido y robado un gran lote de archivos internos

de la empresa fintech. La empresa afirma que el atacante no desplegó *malware* ni manipuló archivos de clientes. Los datos de la empresa se pusieron a la venta en un conocido foro de la dark web.

- **Función secreta de reinicio del iPhone**: Apple ha añadido una función secreta que reinicia los iPhones que no han sido desbloqueados durante un período de tiempo. Los reinicios ponen los dispositivos en un estado donde los datos del teléfono son más difíciles de obtener. La función se añadió en la versión 18.1 de iOS, Esta función fue descubierta por las fuerzas del orden después de que los iPhones de los sospechosos detenidos se reiniciaran misteriosamente mientras estaban bajo custodia. Más información aquí.
- La nueva **detección de estafas en Android se activa**: Google está implementando una nueva función de seguridad en Android que escucha las llamadas y advierte sobre posibles estafas. La función fue anunciada a principios de este año en la conferencia Google I/O. A su vez O2 ha desarrollado un sistema de Inteligencia artificial para hacer perder el tiempo a los estafadores..
- Palo Alto corrige dos vulnerabilidades 0-day en sus firewalls NGFW. La primera, identificada como CVE-2024-0012, CVSSv4 de 9.3 según fabricante, es un fallo de bypass de autenticación que permite a atacantes obtener privilegios administrativos. La segunda se trata de un error que permite una escalada de privilegios a *root*.
- **Importante vulnerabilidad de autenticación en un plugin de WordPress**: Investigadores de seguridad descubren una vulnerabilidad en un **plugin de seguridad de WordPress instalado en más de 4 millones de sitios web**. El error es una omisión de autenticación en ***Really Simple Security*** y **permite a los atacantes acceder a cualquier cuenta en un sitio de WordPress, incluida la de administrador**, debido a un error en el manejo de un *nonce* de inicio de sesión inválido en el procedimiento de 2FA.
  Los investigadores de Wordfence describieron el error como **"una de las vulnerabilidades más serias" que han reportado en los 12 años de historia de la empresa**.
- El Centro de Asuntos del Consumidor **de Japón ha instado a los ciudadanos a planificar su "fin de vida digital"**, recomendando que compartan el acceso a los dispositivos, mantengan listas de contraseñas y **designen herederos digitales** para gestionar las suscripciones.
- Un ciudadano estadounidense de 59 años fue sentenciado a 4 años de prisión por conspiración y espionaje. Ping Li, de Florida, enviaba información al Ministerio de Seguridad del Estado (China) mientras trabajaba para empresas como Verizon e Infosys. Según la sentencia, Li compartió información sobre disidentes chinos, miembros de grupos religiosos de interés en China y ONG con sede en los USA. También compartió información de capacitación (de Verizon y de ciberseguridad) e información sobre el ciberataque de Solarwinds.

DICIEMBRE

- **Piratería de Windows**: Un equipo de crackers de software afirma haber descifrado "*casi todo el esquema de protección de licencias de software de Windows y Office*". Este grupo afirma que su método de elusión puede **funcionar de manera nativa** sin necesidad de software de terceros. El grupo ha probado la técnica para activar licencias de Microsoft Office, Windows 7, Windows 8, todas las ediciones de Windows Server y actualizaciones de seguridad. **Si se confirma, la técnica está destinada a desencadenar un nuevo auge de la piratería de Windows.**

- Ataque a la cadena de suministro: Nuevo ataque que afecta a la librería open-source 'solana-web3.js'. La librería *javascript* se usa para escribir aplicaciones descentralizadas sobre la *blockchain* Solana. El backdoor se introdujo en un commit tras ganar acceso al repositorio a través de ingeniería social, estuvo activo 5 horas y se ocultó en una nueva función addToQueue que enviaba la **clave privada del usuario** en encabezados aparentemente inofensivos a un servidor controlado por el atacante.
- Vulnerabilidad Apache Struts 2: En 2017, una grave vulnerabilidad en el mencionado software permitía ejecutar comandos del con tan solo una petición http sin estar autenticado. Este diciembre, una **nueva vulnerabilidad crítica ha sido parcheada. Permitiría subir cualquier tipo de archivo al servidor, lo que se traduce en ejecución remota de código arbitrario a través de una *webshell***. El fallo posee el CVE-2024-53677 y un score de 9.8/10.
- **¿Demandas para mejorar la seguridad?:** Se ha visto un auge en el uso de la Ley de Reclamaciones Falsas de los Estados Unidos (*False Claims Act*), una normativa que data de la guerra civil americana, para **ganar grandes sumas de dinero demandando a empresas que no cumplen con las obligaciones de seguridad establecidas en los contratos del gobierno federal**. Fomentar estas demandas es una estrategia del gobierno para desalentar las prácticas de seguridad negligentes.
- **Nuevo centro cibernético de la OTAN**: La OTAN combinará tres ramas cibernéticas en un nuevo **centro de coordinación cibernética**. El nuevo Centro Integrado de Defensa Cibernética de la OTAN se lanzará en **2028 y estará ubicado en Mons, Bélgica**. Unificará los roles del Centro de Seguridad Cibernética de la OTAN, el Centro de Operaciones Cibernéticas de la OTAN y la Rama de Análisis de Amenazas Cibernéticas de la alianza.
- Fuerza bruta contra el MFA de Microsoft Azure. Investigadores de Oasis Security descubrieron una vulnerabilidad en uno de los métodos de MFA para Microsoft Azure. Dicho endpoint no implementaba correctamente ***rate-limiting*** limitación de tasa y el período de autenticación duraba tres minutos completos en lugar de los 30 segundos recomendados. Por lo tanto, un atacante podría realizar rápidamente muchos intentos de autenticación simultáneos para enumerar todo el espacio de 6 dígitos del MFA y lograr el acceso.
- La Dirección Nacional de Ciberseguridad de Rumanía afirmó que la banda de ransomware “Lynx” atacó a Eléctrica Group, uno de los mayores proveedores de electricidad del país. Además, reveló que se registraron más de 85.000 ciberataques contra la infraestructura electoral del país entre el periodo electoral del 19 al 25 de noviembre.

MÓVILES

Apple iOS

Las nuevas mejoras de seguridad de iOS 18

Como es habitual en el segundo semestre del año, Apple publicó la versión 18 de su sistema operativo móvil, iOS, en septiembre. Veamos sus mejoras en el aspecto de seguridad.

La primera que llama la atención es la posibilidad de bloquear aplicaciones y usar Face ID (reconocimiento facial) para su desbloqueo.

Una medida de seguridad adicional que mejora la privacidad de las aplicaciones para evitar que se fisgonee en ellas cuando nuestro terminal está desbloqueado y es usado por terceros.

Los usuarios de iOS 18 podrán grabar sus llamadas telefónicas de forma opcional. De hacerlo, el iPhone notificará al otro interlocutor de que la llamada va a ser grabada. Esta característica, por razones legales, no estará disponible en todos los países.

Además de la grabación, podremos obtener una transcripción de la conversación directamente en la aplicación Notas.

Se ha mejorado la granularidad del acceso a contactos por parte de las aplicaciones. Anteriormente solo se permitían dos opciones respecto a este permiso: o se impedía el acceso o se daba acceso completo a la lista de contactos.

A partir de iOS 18, se podrá realizar una selección de contactos permitidos para el acceso por parte de una aplicación que solicite dicho permiso.

También se ha mejorado el acceso y privacidad de los permisos respecto al Bluetooth. En este sentido, el acceso a Bluetooth se limita y es mostrado al usuario para evitar usos abusivos posteriores al pareo entre dispositivos y aplicaciones.

Se introduce una aplicación para gestionar las contraseñas con la capacidad de sincronizarla entre dispositivos e incluso compartir contraseñas con nuestros contactos o familia.

Vulnerabilidades y versiones publicadas en el segundo semestre de 2024

Aunque el verano comenzó relativamente tranquilo en los cuarteles generales de Apple, el día 29 de julio se publicaron nuevas actualizaciones para prácticamente toda la gama de productos de primera línea de la firma californiana.

iOS, por partida doble, vio actualizada la versión 16.7 con la revisión 16.7.9 mientras que la rama 17 ascendió a la 17.6.

Entre los dos paquetes de actualizaciones suman 42 vulnerabilidades corregidas con un impacto variado, desde fugas de información a denegación de servicio.

Poco después, el 7 de agosto se libera una pequeña actualización para las dos ramas: 16.7.10 y 17.6.1, pero no incluyen ninguna actualización de seguridad.

Nos tenemos que remontar casi al final del verano, el 16 de septiembre, para recibir a la revisión mayor, la 17.7 con, precisamente, 17 vulnerabilidades parcheadas.

Ese mismo día, se estrena iOS 18. Además de las novedades que trae, viene con 40 correcciones de seguridad. Llama la atención que, lejos de vulnerabilidades de corrupción de memoria, muchos fallos son por defectos de controles de seguridad que pueden ser evadidos o fallos lógicos que pueden ser aprovechados para un fin distinto, y malicioso, al pretendido.

Semanas después se desliza una pequeña pero curiosa actualización, la revisión 18.0.1. Dos fallos corregidos: el primero es debido a que es posible realizar una grabación de audio de segundos antes de que el indicador de captura de audio (círculo ámbar) se active.

La segunda es algo más curiosa aún. Se corrige un fallo por el cual un atacante podría "escuchar" las contraseñas guardadas en el dispositivo debido a un uso abusivo de la característica de accesibilidad "VoiceOver".

Nos vamos a finales de octubre, el 28 concretamente. Ese día se publica 17.7.1 y esta nos repara 23 fallos de seguridad. 23 fallos que es casi la mitad que corrige iOS 18.1 el mismo día: hasta 55 parches, nada más y nada menos. Un gran lote que incluye peligrosas vulnerabilidades corregidas, tales como una ejecución de código arbitrario en el IOSMobileFrameBuffer, el componente encargado de renderizar la pantalla del iPhone.

19 de noviembre, Apple publica dos revisiones menores: la 17.7.2 y 18.1.1. Ambas corrigen los mismos errores de seguridad que afectan a Webkit y no solo son peligrosos (conllevan ejecución de código arbitrario al visitar contenido web) sino que están siendo activamente explotados.

Y cerramos 2024 con dos grandes parches. El 19 de diciembre se publica 17.7.3 con 26 correcciones y la 18.2, gran revisión de la versión 18 que contiene hasta 32 vulnerabilidades parcheadas.

Evolución de vulnerabilidades en iOS durante el segundo semestre de 2024

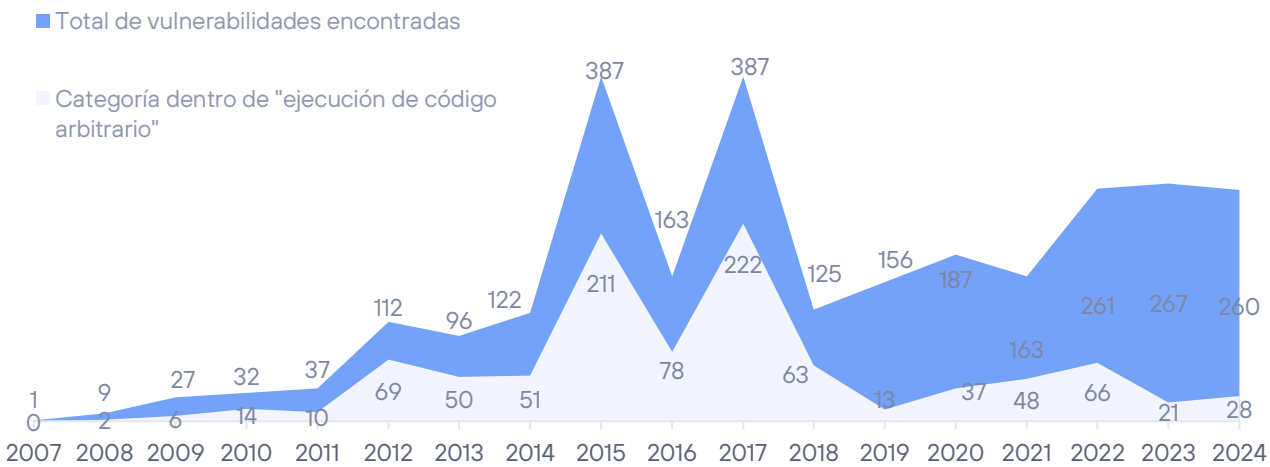
El segundo semestre de 2024 se ha cerrado con 149 vulnerabilidades únicas parcheadas, cuatro consideradas de alto riesgo, con posibilidad de ejecutar código arbitrario.

En total, en 2024, se han corregido 260 vulnerabilidades. Lo que representa una ligera disminución respecto a las 267 del año anterior. Similar número encontramos en 2022 (261).

La estimación de vulnerabilidades con alto impacto (ejecución de código arbitrario) se eleva a 28, siete más que el año anterior.

VULNERABILIDADES EN IOS 2024-H2

Evolución de vulnerabilidades por año



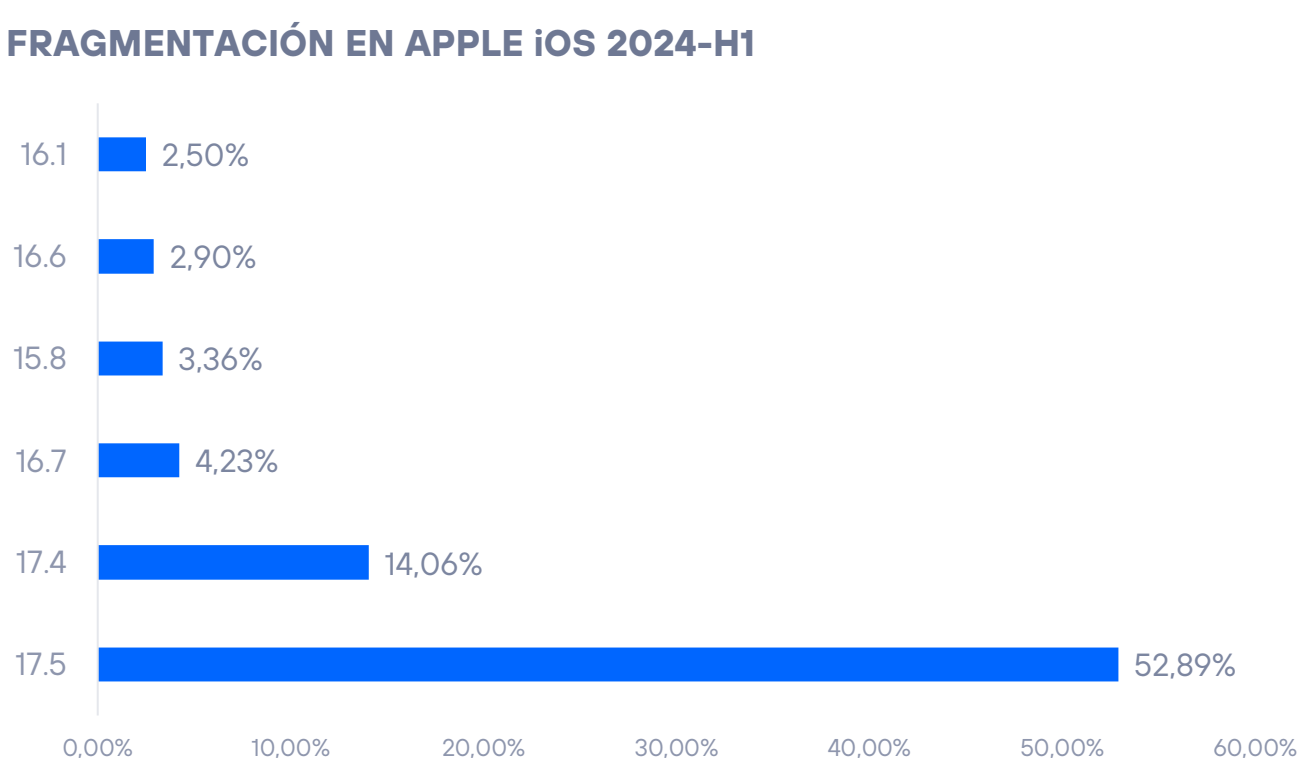
Fragmentación de versiones durante el segundo semestre de 2024

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

La foto del segundo semestre de 2024 nos presenta una fuerte presencia de la nueva versión de iOS, la 18, como es habitual. La liberación de una nueva versión del sistema operativo es un evento esperado por los usuarios de Apple y su actualización, incluso en las primeras horas, es masiva. Es destacable que incluso iOS 18.2, liberada bien traspasado el meridiano de diciembre, llega al 6.57% del parque móvil.

Nos quedamos entonces con la estrenada iOS 18 que posee un pequeño porcentaje, 4.31% debido a que el grueso de la población 18 está ahora en la 18.1, con prácticamente un 50%. Sumamos la ya comentada iOS 18.2 con el 6.57% lo que nos da algo más del 60% de adopción.

La rama anterior, iOS 17 suma 10.95% de 17.6 y un 3.5% de 17.5. La rama 16 pervive con un modesto 3.46%, limitada a terminales como iPhone 8 con casi ocho años de antigüedad.



Android

Nuevas características de seguridad

El 15 de octubre salió al público Android 15. Vamos a ver qué novedades de seguridad implementa esta nueva iteración del sistema operativo móvil de Google.

Una de las novedades es la protección por robo. Es interesante porque no se trata solo de un bloqueo del terminal de forma remota, el cual puede hacerse desde otro terminal usando una verificación de seguridad. Android implementa un sistema que detecta el robo físico del terminal en "vivo". Es decir, que alguien robe el terminal y salga corriendo. En semejante escenario, el sistema detectará que algo raro pasa y bloqueará el terminal para evitar su manipulación.

Además de físicamente, también posee una heurística que trata de averiguar si el móvil está siendo manipulado para acceder a información o cambiar sus características: manipulación de la SIM, acceso reiterado fallido a contraseñas, cambios en ciertos parámetros de la configuración o si el terminal está desconectado de las redes (móviles o wifi conocidas) etc. En tales casos, el terminal también se bloqueará.

Respecto de la privacidad, se ha implementado una nueva característica denominada "espacio privado" que consiste en la creación a demanda de un grupo de aplicaciones que queramos ocultar de la vista. No solo se ocultará el icono de la aplicación sino también sus notificaciones o la configuración de estas. Además, podremos ocultar el propio espacio privado a la vista de los demás. Todo esto está pensado por si el terminal es usado discrecionalmente por terceros o se encuentra desbloqueado.

Continuando con el capítulo de la seguridad, la versión 15 implementa una función avanzada de ocultamiento de ciertas aplicaciones cuando se está compartiendo pantalla. Por ejemplo, ciertas notificaciones no podrán verse en pantalla compartida y de hecho, solo se podrá ver la aplicación a compartir y no todo el sistema. Además, si el sistema detecta que va a visualizarse una contraseña, una tarjeta de crédito o datos de inicio de sesión, se ocultarán y no podrán ser vistos mientras se usa la función de compartir pantalla.

Cerrando el capítulo de seguridad, Android 15 implementa mejoras en el gestor de contraseñas, nuevas características de seguridad disponibles en la API para programadores, robustecimiento de algunos "Intents" y mejoras en la privacidad de algunas características.

Vulnerabilidades

Android publica un conjunto de parches cada mes, generalmente durante la primera semana. En este segundo semestre de 2024 se han publicado seis boletines con la siguiente distribución de vulnerabilidades por cada mes:

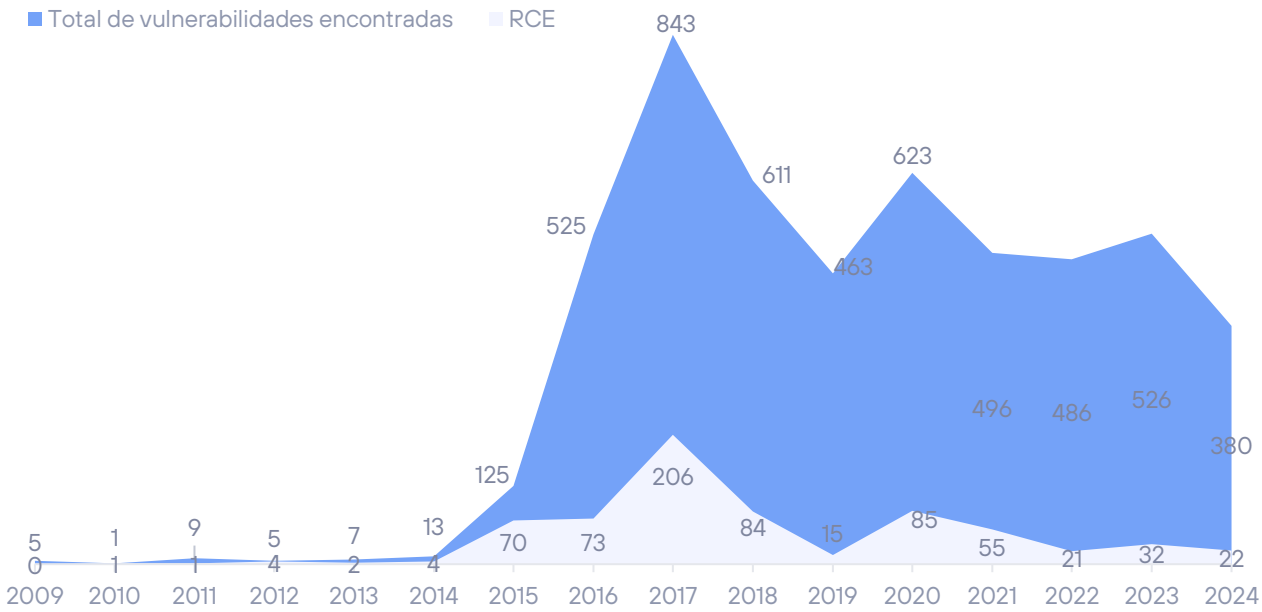
Mes	CVEs	Críticos o RCE
Julio	16	2
Agosto	40	2
Septiembre	35	2
Octubre	24	1
Noviembre	38	2
Diciembre	14	1

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, 167 parches en este semestre (el semestre anterior fue de 213); 10 de ellos considerados críticos (12 en el semestre anterior). Lo que hace un total en 2024 de 380 vulnerabilidades corregidas.

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

VULNERABILIDADES EN ANDROID 2024-H2
Evolución de vulnerabilidades por año



Fragmentación en sistemas Android

La última publicación de *Statcounter* a fecha de edición de este informe nos indican que la versión más implantada de Android es la 14, con un share que supera al 25.64% del semestre pasado con un 36.95%, seguida por la 13 con un share del 18.81% que desciende desde el 22.29%.

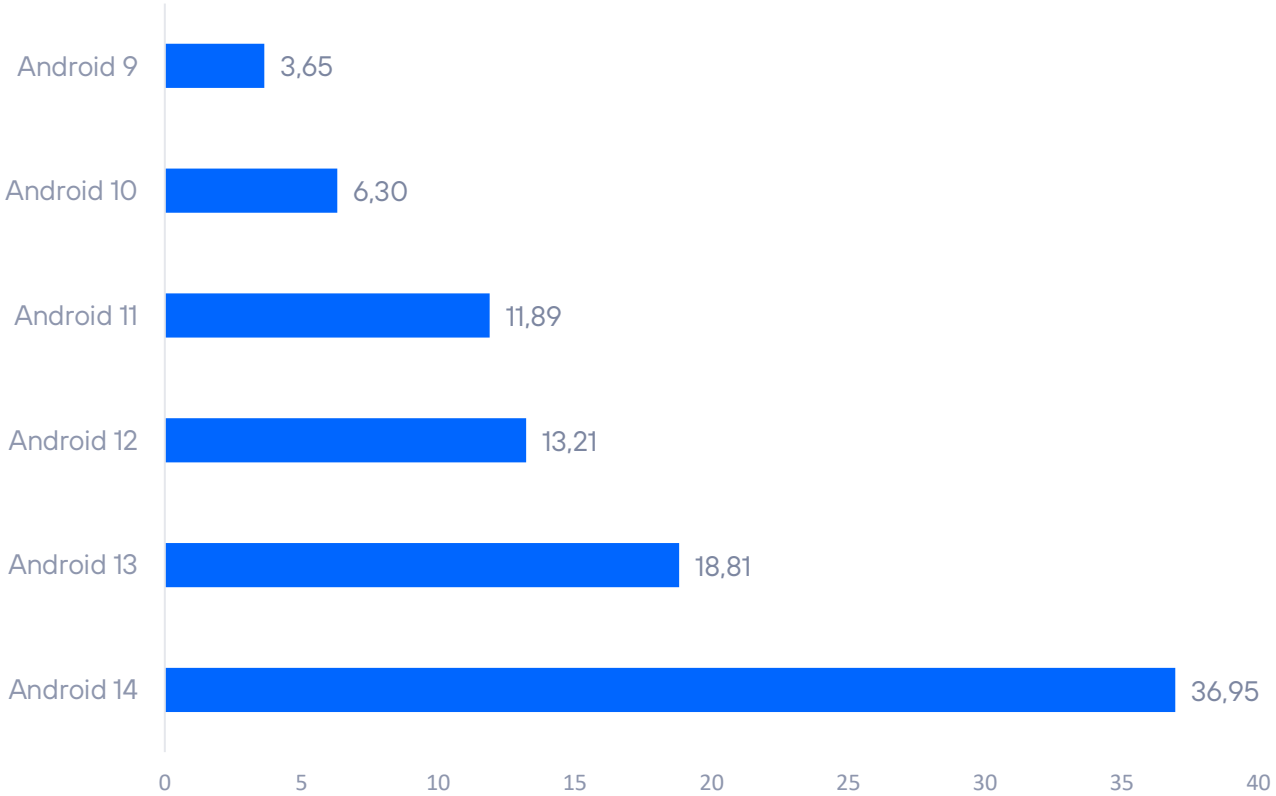
Android 15 aún no ha tenido un efecto notable en el parque de dispositivos móviles de dicho sistema. Habrá que esperar a la nueva edición de este informe para evaluar la situación. Es notable incluso el aumento en cifras de la versión anterior, la 14, que ha crecido incluso en penetración.

Entra dentro de lo normal, puesto que una nueva versión, publicada a finales de verano, tarda en hacerse con un hueco. Además de que el conteo de cifras también hace que la ventana de exposición de nuevos modelos tarde en aparecer.

Las versiones de Android anteriores a la versión 12 (incluida, sistema que apareció en septiembre de 2020) ya no tienen soporte de actualizaciones. Aun así, cuentan con notables cifras: Android 11 un 11.89%, Android 10 un 6.30% y cerrando la cola, Android 9 con un 3.65%.

Hay un 10% no contabilizado que puede estar tanto consolidado por versiones incluso más antiguas, pero ya no entran dentro del casillero para su clasificación. Estaríamos hablando de un parque de casi el 25% de terminales con sistemas operativos sin soporte alguno, lo que hace que estén expuestos a vulnerabilidades y su explotación.

FRAGMENTACIÓN EN ANDROID 2024-H2



VULNERABILIDADES DESTACABLES

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

CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2024-6385,	Gitlab	Un fallo en Gitlab permite ejecutar trabajos como otro usuario.	9,6
CVE-2024-20401	Cisco	Ejecución de código a través de un problema de “path traversal”	9,8
CVE-2024-4879	ServiceNow	A través del encadenado de varios fallos, se podría obtener control total del sistema	9.3
CVE-2024-29847	Ivanti	Un problema en la deserialización permite la ejecución de códito	10
CVE-2024-6678	Gitlab	Un fallo en Gitlab permite ejecutar trabajos como otro usuario.	9,9
CVE-2024-8963	Ivanti	Path Traversal en Ivanti CSA permite que un atacante remoto no autenticado acceda a funcionalidad restringida.	9.4
CVE-2024-7593	Ivanti	Un fallo en la autenticación permite acceso no restringido al panel de administración	9.8
CVE-2024-38812 **CVE-2024-38813**	VMware vCenter	Ejecución de código en con la concatenación de dos vulnerabilidades.	9.8
CVE-2024-29824	Ivanti	SQL injection en Endpoint Manager	9.6
CVE-2024-23113	Fortinet	Ejecución de código en FortiOS	9.8

CVE-2024-9486	Kubernetes	Fallo en SSH permite acceso no autenticado a las máquinas virtuales	9.8
CVE-2024-47575	Fortinet	Un problema en la API de FortinetManager permite ejecución de código	9.8
CVE-2024-20418	Cisco	Ejecución de código en los puntos de acceso Ultra-Reliable Wireless Backhaul (URWB).	10
CVE-2024-0012.	PaloAlto	Una omisión de autenticación en el software PAN-OS de Palo Alto Networks permite que un atacante no autenticado con acceso a la red a la interfaz web de administración	9.8
CVE-2024-11639	Ivanti	Acceso administrativo a la consola de Ïvanti CSA	10
CVE-2024-53677	Apache Struts	Un fallo de path traversal permite subir ficheros arbitrarios y ejecución de código.	9.6
CVE-2023-34990,	FortiNet	Ejecución de código en FortiVLM	9.8
CVE-2024-34026	OpenPLC	Una solicitud Ethernet/IP especialmente diseñada puede provocar la ejecución remota de código. Un atacante puede enviar una serie de solicitudes para activar esta vulnerabilidad.	9.8
CVE-2024-4708	mySCADA	mySCADA myPRO utiliza una contraseña codificada ("hard-coded") que podría permitir a un atacante ejecutar código de forma remota en el dispositivo afectado.	9.3
CVE-2024-8956	Cámaras de ValueHD	Las cámaras PTZOptics PT30X-SDI/NDI-xx anteriores al firmware 6.3.40 son vulnerables a un problema de autenticación insuficiente. La cámara no aplica correctamente la autenticación cuando se envían solicitudes sin el encabezado HTTP "Authorization". Un atacante remoto y no autenticado puede filtrar datos confidenciales y actualizar valores de configuración individuales o sobrescribir todo el archivo.	9.1

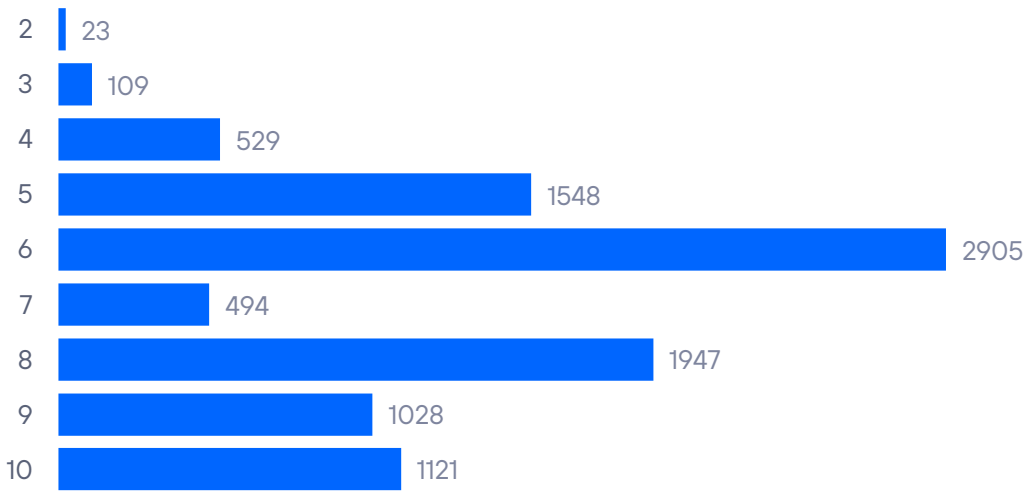
CVE-2024-8497	Franklin Fueling Systems	Las versiones de Franklin Fueling Systems TS-550 EVO anteriores a 2.26.4.8967 poseen un archivo que puede leerse arbitrariamente y que podría permitir a un atacante obtener credenciales de administrador.	8.7
CVE-2024-8630	Consola para tanques de estaciones de servicio Sibylla	Una inyección de SQL exitosa podría dar como resultado que un atacante obtenga información del dispositivo de la base de datos, elimine credenciales o potencialmente obtenga acceso de administrador	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

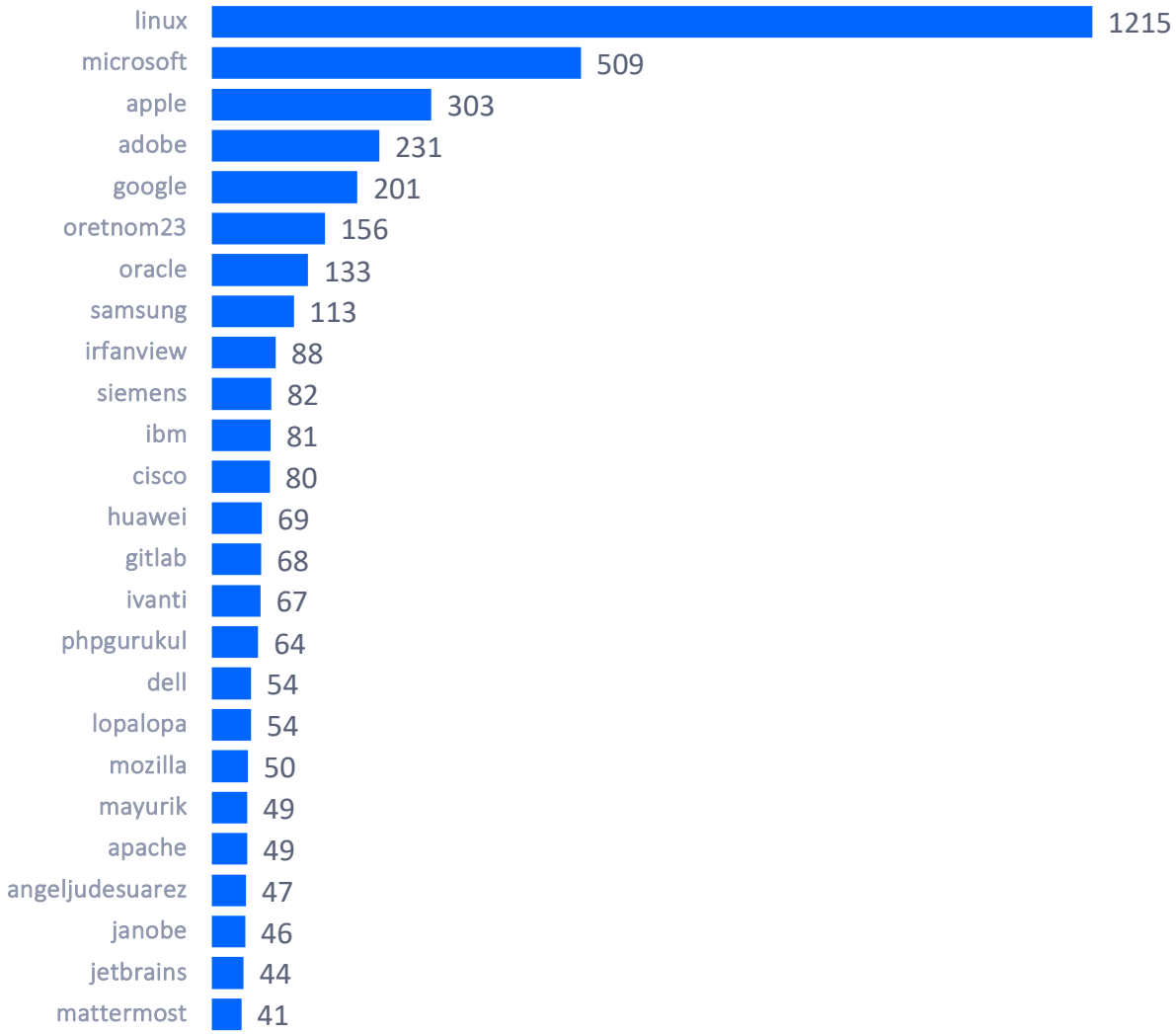


Top 25 compañías con más CVE acumulados

Durante el segundo semestre de 2024, Linux ha liderado con diferencia por número de vulnerabilidades conocidas, seguido de Microsoft y Apple. En general, es habitual que Microsoft, Adobe, Google y Oracle estén siempre entre los primeros en número de vulnerabilidades. No hemos encontrado una razón concreta pública por la que se hayan reportado tantos CVEs asociados a Linux en este semestre.

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 2024

Venomous Bear – Sin honor entre APT-Groups

También conocido como “Turla”, este grupo lleva activo al menos 20 años y está respaldado por el FSB, según indica el DOJ de los USA (ya tenemos bastantes acrónimos en una frase). Pese a que han sido “desarticulados” varias veces, tienen una capacidad de resiliencia mayor que los sistemas que atacan.

En este caso, han sido vistos atacando objetivos en Ucrania, pero utilizando plataformas y posiciones desplegadas por otros grupos. Por ejemplo, por los “Mythic Leopard” paquistaníes. Al parecer, el oso accedió a redes ya controladas por el leopardo en Afganistán e India, y modificó los servidores C2 de éstos para utilizarlos en sus andanzas.

No parece que el grupo paquistaní sea el único que ha sido envenenado por este oso.

Hay quien afirma que son los responsables de la campaña de espionaje (y correspondiente brecha) Moonlight Maze, lo que situaría su existencia en 1996 al menos.

Más información en https://www.bleepingcomputer.com/news/security/russian-hackers-hijack-pakistani-hackers-servers-for-their-own-attacks/

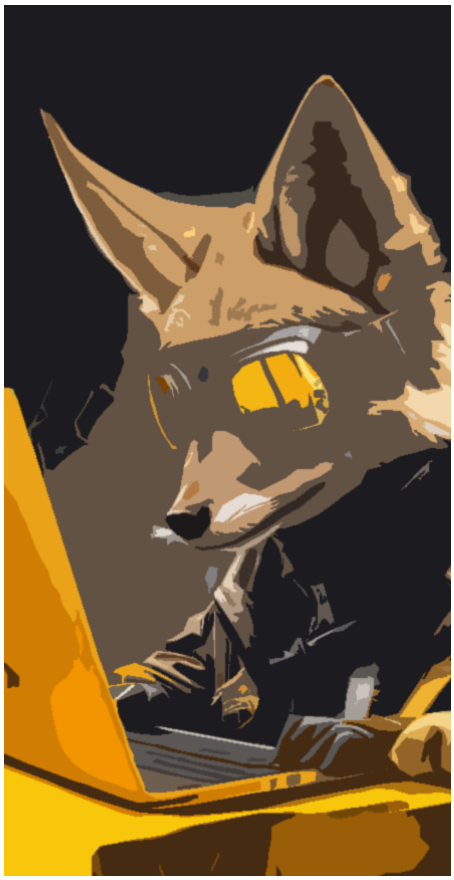
Golden Jackal – Rompiendo las leyes de la física

De este grupo ya hablamos en el informe del primer semestre de 2023. Varios investigadores de We Live Security han detectado al chacal saltándose el supuestamente infalible "Air-gap" de varios sistemas gubernamentales europeos.

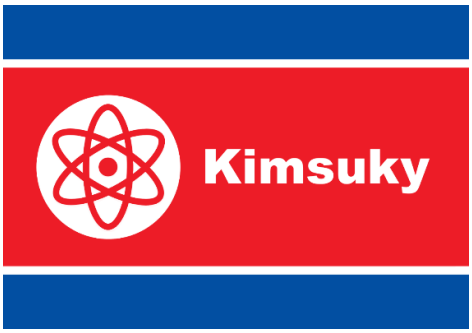
Su objetivo preferido sigue siendo la información: direcciones de e-mail, claves de cifrado, ficheros... Sin embargo, los investigadores no revelaron quién (quiénes) fue exactamente su objetivo.

No vamos a relatar cómo se preparan y ejecutan estos ataques para vulnerar redes aisladas, porque nos llevaría unas 52 páginas, pero digamos que no es precisamente sencillo y requiere en muchos casos de negligencia o colaboración por parte de las potenciales víctimas.

Sigue sin ser posible relacionar a este grupo con un país concreto, aunque siguen empleando algunas expresiones que recuerdan a nuestro amigo el oso de más arriba...



Más información en: https://www.welivesecurity.com/en/eset-research/mind-air-gap-goldenjackal-gooses-government-guardrails/



Kimsuky – Vuelta a los estudios

Este grupo norcoreano ha sido relacionado con varios ataques dirigidos a profesores e investigadores universitarios de Corea del Sur.

Relacionados siempre con el Spear Phishing y la ingeniería social, fueron detectados al cometer un error (seguramente) en el exfiltrado de la información. Gracias a esto, se pudo saber cuales eran sus TTP.

Una de ellas es la ejecución de su trabajo con herramientas ofuscadas para volar por debajo del radar de las empresas de hosting. Entre sus herramientas destaca el uso de un webshell llamado "GreenDinosaur" para operar en el host que han tomado.

Teniendo en cuenta que lo suyo es el robo de información de investigación (nuclear, farmacéutica, médica...), cuando se los detecta relacionados con delitos financieros es porque esa es su manera de financiar el resto de su trabajo.

Más información en: https://thehackernews.com/2024/08/university-professors-targeted-by-north.html

Sandman - La arena se cuela por todos lados

- *Duerme con un ojo Abierto*
- *Agarrando tu almohada con fuerza…*

Porque el hombre de arena ha aprendido a colarse en tus sistemas aprovechando los túneles de Vistual Studio Code, el editor de código fuente de Microsoft.

Al parecer, este grupo, vinculado con China, habría sido detectado colándose en proveedores europeos de servicios de TI empleando VSCode para mantener su acceso persistentemente. Y decimos "habría sido" porque no se tiene certeza sobre el autor de esta actividad.

Estos túneles se establecen a través de Azure con ejecutables firmados por Microsoft y sirven para trabajar de manera segura (…) en sistemas remotos.

Al parecer, el vector de entrada es la explotación de un típico SQLi. Una vez establecido el acceso, despliegan un webshell y… a jugar.

Al desplegar VSCode y configurar los túneles no hacen nada "ilegítimo" por lo que las herramientas de seguridad no detectan actividad maliciosa.

Esta táctica no es nueva pero sí es rara. En septiembre de este mismo año, el grupo chino "Mustang Panda" fue detectado empleando la misma estrategia.

¿Mismo panda, pero con distinto collar? Ya veremos.

Más información en: https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/

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.

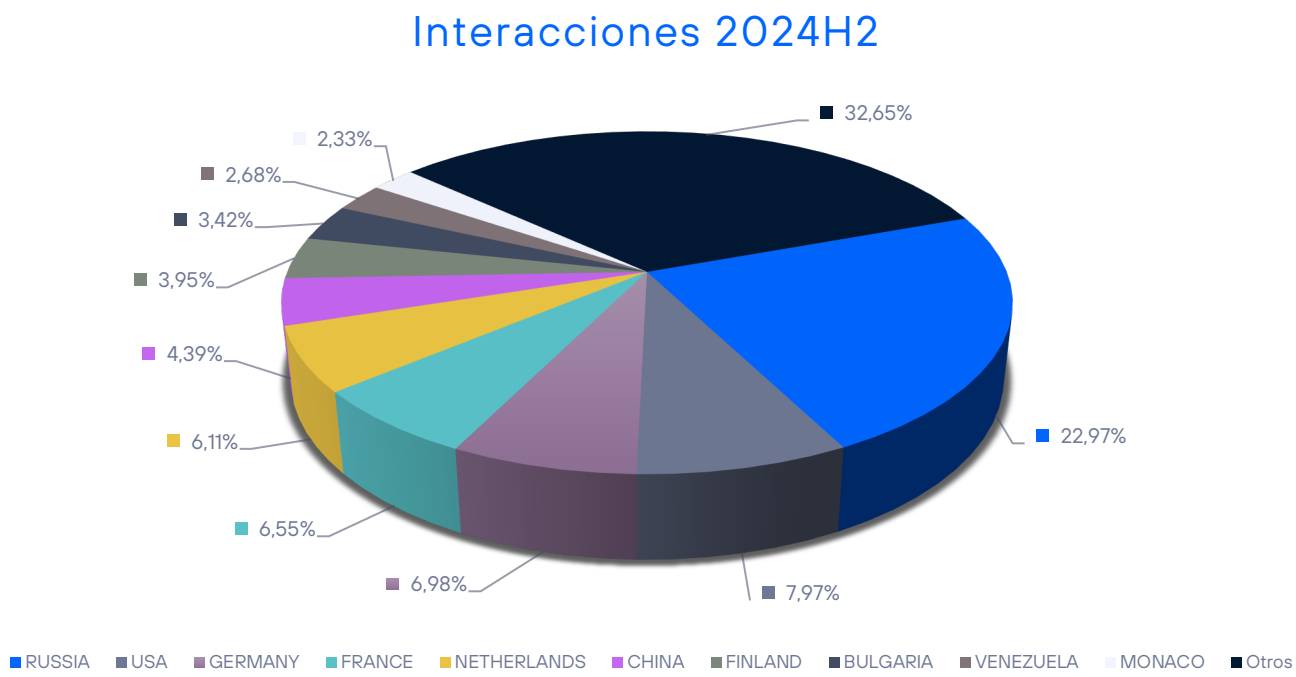
Análisis de la información

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.

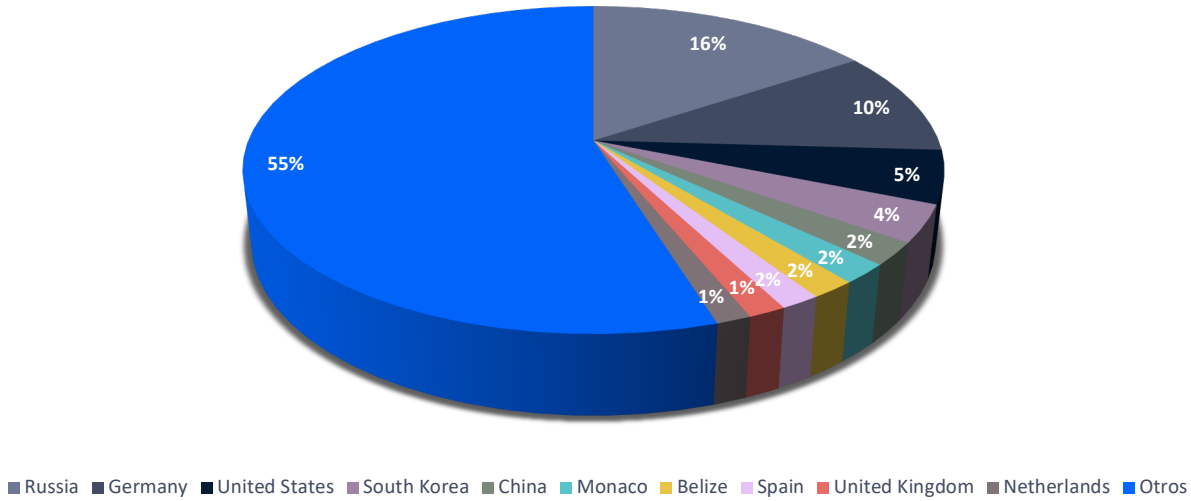
- Asociación de eventos y acciones en eventos complejos: esto conlleva que el número total de eventos disminuya. Se contabiliza menos actividad, aunque se registre la misma (o más). Por ejemplo, 100 intentos de acceso por RDP a un PC de control desde la misma IP en un lapso corto de tiempo pasa a contar "1" (RDP bruteforce) en lugar de contar el número de intentos de acceso a través de RDP, 100. De hecho, si fueran 250 intentos, también contaría como 1. Es cierto que se pierde la medida "gruesa", pero al fin y al cabo lo importante no es el dato global (que, por supuesto, conservamos y podemos tratar con él) ya que un sistema automatizado puede hacer 100 o 1000 intentos en un ataque y en realidad sigue siendo un mismo atacante ejecutando una misma acción con las mismas TTP (tácticas, técnicas y procedimientos) y los mismos IoA e IoC.
- Identificación de interacciones "grises": Aristeo ya diferenciaba de manera binaria entre actividad legítima y aquella que no lo era (blanco/negro). Ahora, es capaz de identificar aquellas interacciones que no tienen por qué ser maliciosas por sí mismas, pero que tampoco son legítimas o solicitadas. Por ejemplo, tráfico generado por metabuscadores o servicios de seguridad de empresas. Esta diferenciación permite seguir archivando la información "gris" para trabajar con ella, pero enfocando la actividad de Aristeo y de los analistas hacia los eventos que no provienen de este tipo de servicios o instituciones, si no de auténticos atacantes.
- Más granularidad en la información ya existente, lo que equivale a más información para tratar: la capacidad para discernir actividad por sus orígenes o para agruparla permite también trabajar mejor con la información que se estaba generando y generar más de ésta. Aristeo puede ahora identificar con más facilidad los eventos de ciberseguridad que ocurren y situarlos en un contexto entendible para un analista, como por ejemplo las **matrices Enterprise e ICS de MITRE**.
- Mejora en la lectura de actividad en toda la red: Aristeo tenía un sesgo hacia la actividad recibida en España, debido a que sus señuelos se posicionan mayoritariamente en su país de nacimiento. Hemos introducido cambios para registrar más información a través de todo el mundo, lo que implica más profundidad y amplitud en el registro de la actividad atacante.

Pasamos a la estadística general de la información registrada. En el segundo semestre de 2024 se detectaron **más de 333 millones de eventos de ciberseguridad, pero con la nueva versión, en la que se agrupan eventos en otros más complejos, la cifra disminuye. Estaríamos hablando, por lo tanto, de más de 27 millones de eventos complejos en el semestre con el nuevo sistema de conteo**. Comparando las cifras obtenidas con la misma versión, esto supone un ascenso respecto a los datos registrados en el primer semestre de 2024, 313 millones, y un pequeño ascenso respecto al segundo trimestre de 2023, cuando se registraron unos 322 millones de eventos. No obstante, las cifras se mantienen en rangos muy similares, por lo que se podría decir que la situación permanece estable.

La distribución por países sería la siguiente:



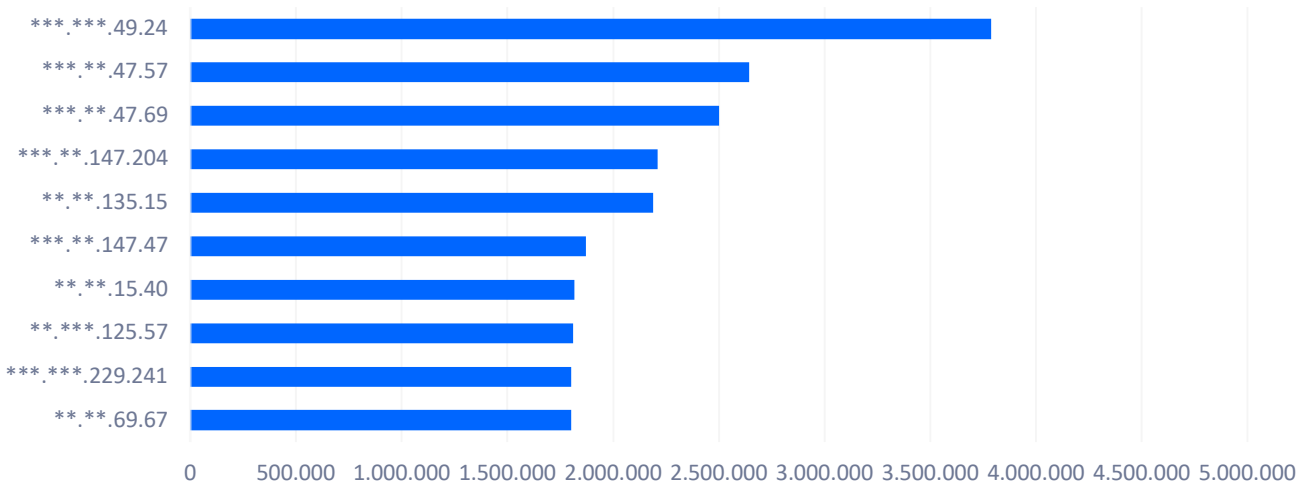
Interacciones 2024-H1



Como se puede observar, pese a haber aumentado la amplitud de la red de Aristeo, los países con más interacciones hacia los señuelos siguen siendo viejos conocidos. Pese a que pueda haber una leve variación en los países registrados, si se busca el histórico de todos los semestres (y con el acceso a todos los datos que tenemos) se puede concluir que la situación es muy similar. Sobre todo si, además de a los países, observamos las regiones del mundo que ocupan.

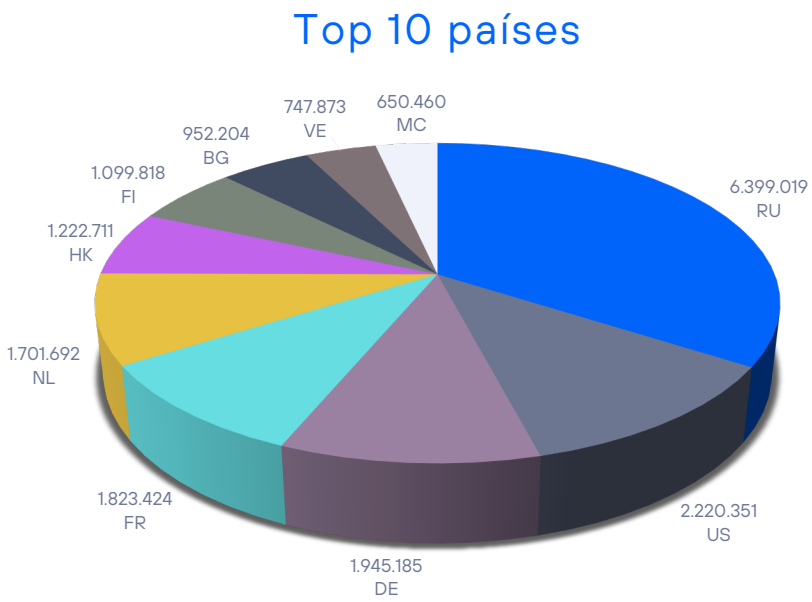
Ahora vamos a ver las diez direcciones IP con más interacción con el sistema de Aristeo. En este semestre, igual que durante el anterior, la gran mayoría de direcciones IP de este Top-10 proviene del centro-norte-este de Europa. Sin embargo, la cantidad no es el 85% como en el semestre anterior. En este caso, la dirección IP con más actividad no es europea y se cuelan en el Top-10 otras direcciones que tampoco lo son. Seguramente este dato esté relacionado también con la mayor amplitud de la red de Aristeo. Al posicionarlo mejor respecto al mundo, hemos conseguido capturar información más precisa en referencia al panorama mundial.

TOP-10 IP atacantes



También se puede observar un descenso del total de eventos que representan las direcciones IP del Top-10. Esto también tiene que ver con la mayor capacidad de registro. Al registrar más direcciones IP, con un número de interacciones similar, el total se divide entre más actores y el Top-10 pierde representatividad.

A continuación, vemos cómo se reparten el *top 10* de los países registrados. Este semestre desaparece España como país (del Top-10, pero sigue en el Top-30). 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.



También se observa que la cifra de eventos es mucho menor que la del semestre pasado. La razón es, recordemos, que los eventos ahora se agrupan en eventos complejos y por lo tanto las cifras son distintas porque no miden lo mismo.

Sirva este apartado para cerrar el análisis con la versión 1.0 de Aristeo. El semestre que viene añadiremos los gráficos de la versión 2.0.

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: 359.529 direcciones IP, 73.838 dominios y 565.583 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	442300	78,20%
Phishing	114590	20,26%
Strela Stealer	3300	0,58%
Lumma Stealer	1952	0,35%
FAKESUPDATES	1057	0,19%
malware	907	0,16%
Mozi	621	0,11%
DCRat	604	0,11%

Coper	476	0,08%
NetSupportManager RAT	390	0,07%

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.

Mención especial a un malware que ha golpeado especialmente a países como España, Ucrania y Alemania a finales de 2024: Strela Stealer. Como veremos en la parte de dominios, ha copado titulares en la prensa especializada y sus efectos se han dejado ver y notar.

Strela usa como vector el phishing a través de correos electrónicos haciéndose pasar por servicios bancarios entre otros disfraces. A través de dicho phishing se realiza una descarga de malware curiosamente firmado digitalmente con un certificado robado a una empresa brasileña.

Salvando las categorías genéricas, 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.

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

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

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

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

pages.dev	6663	1,18%
github.io	5788	1,02%
vercel.app	5676	1,00%
farpetor.shop	4882	0,86%

lameshamer.shop	4882	0,86%
geriguna.shop	4882	0,86%
gerlia.shop	4882	0,86%
gloomcutter.shop	4882	0,86%
glynnorin.shop	4882	0,86%
gonnhild.shop	4882	0,86%

Como es habitual, los primeros puestos pertenecen a servicios online que permiten alojar de forma gratuita contenido web: pages.dev, github.io, vercel.app. Tras ellos, vienen los dominios usados por campañas individuales, en particular, ese número (4882) no es un error sino un grupo de dominios (unos miles muy concretos captados en la base de datos) que se asocian a un grupo de campañas relacionadas con el malware Strela, del que ya hemos hablado antes.

La difusión de dicho malware ha sido especialmente aguda con dominios del tld ".shop". Tanto registros indiscriminados como tiendas online que han sido objeto de intrusión por parte del grupo criminal tras las campañas de diseminación de este malware.

¿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	53727	14,94%
India	49806	13,85%
China	37670	10,48%
Vietnam	22633	6,30%
Rusia	13843	3,85%

Alemania	11021	3,07%
Corea del Sur	10747	2,99%
Taiwan	10536	2,93%
Pakistan	10476	2,91%
Brasil	8352	2,32%

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	155191	43,17%
HTTP Spammer	140821	39,17%
Mail Spammer	131096	36,46%
Malicious host	91431	25,43%
SSH Attacker	45292	12,60%
Proxy	33936	9,44%
Bruteforce	31380	8,73%
Port Scanner	30032	8,35%
Host scanner	27226	7,57%

Hacking	26583	7,39%

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 casi 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% 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 9%.

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 9.5% 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 7.39% 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	16511	40,46%
dev	5997	14,70%
top	3613	8,85%
app	3350	8,21%
io	2782	6,82%
my.id	2292	5,62%
org	1852	4,54%
net	1578	3,87%
xyz	1438	3,52%
sn	1394	3,42%

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

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

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

¿Qué categorización maliciosa poseen los dominios estudiados?

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

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

Phishing	48753	66,03%
Metastealer	6960	9,43%
Virut	5756	7,80%
Malware download	1974	2,67%
Lumma Stealer	1810	2,45%
CryptBot	1408	1,91%
Malware	1132	1,53%
Hook	826	1,12%
Astaroth	477	0,65%
FAKEUPDATES	416	0,56%

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.

CONCLUSIONES DEL INFORME

En la mitad segunda mitad de 2024 se confirma que se superan el número de vulnerabilidades que permiten la ejecución de código en iPhone con respecto a 2023, si bien se han frenado en el segundo semestre, y finalmente son 28. En **Android, al contrario, se reducen considerablemente tanto las las vulnerabilidades en general como las graves en particular**. Si en 2023 fueron 32, en 2024, cuentan con 22 críticas.

Si Oracle, Microsoft y Google son las empresas con más fallos corregidos habitualmente, este semestre se cuela Linux por todo lo alto con 1200 vulnerabilidades. No hemos podido encontrar una razón concreta pública para este aumento de correcciones en la base de datos consultada.

Con respecto a Aristeo, estrenamos versión 2.0 con muchas novedades que modifican la fórmula en la que se contabilizan los eventos e incidentes. También se amplía la capacidad de captación en otros países. En este semestre, igual que durante el anterior, la gran mayoría de direcciones IP de este Top-10 proviene del centro-norte-este de Europa. Sin embargo, la cantidad no es el 85% como en el semestre anterior. En este caso, la dirección IP con más actividad no es europea y se cuelan en el Top-10 otras direcciones que tampoco lo son.

Una campaña bastante potente del malware Strela Stealer se cuela en el top 3 de malware alojado en Internet junto con los más genéricos “malware” y “phishing.

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

¡Ja! Fingerprinting de cifrado, ¿no?

Comunicación y prensa: cobertura mediática de incidentes y ciberataques

Carteras digitales: máxima usabilidad, ¿máxima seguridad?

Incidente Digicert, o cuando una revocación de certificados termina en pleito

INTELIGENCIA ARTIFICIAL

Project Zero, descubrimiento de vulnerabilidades usando modelos LLM

Ética en IA y Machine Learning: Las zonas grises de las variables sensibles

MALWARE

El uso de Flutter en el malware para dificultar los análisis