karonte

Diciembre/2023

Tabla de Contenidos

Introducción

¿Quiénes somos?

Este informe ha sido realizado por el departamento de **I+D+i** de **Ewala IT Services SL**[1].

Ewala es una **Empresa Innovadora de Base Tecnológica (EIBT)**. Nuestra sede principal está en Asturias y esto es lo que hacemos:

- Somos especialistas en **Ciberseguridad Industrial (OT)** y **Ciberseguridad IT**.
- Desarrollamos nuestras propias herramientas (**Threat Intelligence**, **Asset Monitoring**, etc.) gracias a nuestro departamento de I+D+i.
- Ofrecemos servicios de ciberseguridad 100% personalizados, y con ello la mejor solución adaptada en cada caso.
- Desde nuestro departamento financiero asesoramos a los clientes en la financiación de cada proyecto.

[1] https://www.ewala.es/

¿Qué son los Data Leaks?

La **hiperconectividad** por parte de las empresas favorece la innovación tecnológica y sus transiciones hacia modelos productivos más eficientes, mientras que por otro lado aumenta su **exposición** ante los **riesgos digitales**.

Una de las amenazas que mayor impacto reputacional y económico tienen en las organizaciones es el **Data Leak**.

Data Leak es la terminología utilizada para referirse a la **fuga de información**. Se trata, por lo general, de grandes volúmenes de datos que contienen **información confidencial** de empresas o de individuos particulares, y cuyo control ha traspasado las barreras de contención que separan lo privado de lo público, pudiendo localizarse **en foros, redes sociales o en el mercado negro**.

A lo largo de los meses del presente año **2023** se han intercambiado y vendido cuantiosas sumas de **datos críticos** entre los cuales pueden hallarse **cuentas bancarias**, **contraseñas** o **documentación confidencial**.

¿Cómo ocurren las fugas de información?

Existen diversos escenarios que funcionan como detonadores de fugas de datos. Algunos de los casos más habituales a los que se debe prestar especial atención son los siguientes:

Filtración Interna No-intencionada

Detonador:

Un usuario incurre en descuidos continuos a la hora de manipular información confidencial. Desconoce que precauciones de seguridad ha de tener presente a la hora de compartir información con compañeros dentro o fuera de la compañía.

Propagación:

El usuario desprevenido acaba de compartir información mediante

Filtración Interna Malintencionada

Detonador:

Un empleado descontento o con malas intenciones decide capturar información de la empresa para ponerla a disposición pública o a la venta.

Propagación:

El usuario mal intencionado extorsiona a la empresa o publica directamente la información en foros de intercambio de Data Leak o en páginas de compra/venta de datos fugados.

Secuestro Externo de Información

Detonador:

Una empresa cuenta con portales web expuestos a Internet; uno de los portales presenta serias vulnerabilidades de inyección de código, permitiendo ejecutar consultas contra la base de datos.

Propagación:

Un usuario mal intencionado ha localizado la vulnerabilidad antes de que la empresa pudiera detectarla; posteriormente descarga el extracto de la base de datos y lo publica en los foros de intercambio de Data Leaks.

¿Qué impacto tienen?

El impacto de las **fugas de información** puede medirse tanto a nivel **reputacional** como **económico**.

Cuando un usuario mal intencionado adquiere información confidencial de una organización pueden desatarse las siguientes amenazas:

- El usuario mal intencionado pide un **rescate** por los datos filtrados, incurriendo en un delito de **extorsión**.
- El usuario mal intencionado decide comprometer la seguridad de la organización con los datos obtenidos.

La materialización de la **amenaza** puede repercutir negativamente a la **reputación** cuando lo que se ve afectado es la propia **imagen** de la empresa; en esta línea suelen encontrarse filtraciones de cuentas de redes sociales o credenciales corporativas que permiten al usuario mal intencionado suplantar identidades de la organización, realizar campañas de desprestigio con un amplio alcance al público general y capturar así la atención de la prensa.

Por otra parte, el uso mal intencionado de información filtrada a internet puede provocar la **paralización** total o parcial de **servicios críticos** en las organizaciones, así como también cuantiosas e instantáneas **pérdidas financieras** en caso de tratarse de datos bancarios.

Metodología y fuentes

- Los datos mencionados en el presente informe fueron extraídos de la base de datos de **Karont3 Data Leak Observatory**, abarcando el intervalo de tiempo comprendido entre 01/2023 y 12/2023.

- Para el análisis de los datos se ha seguido una metodología cuantitativa rigurosa basado en análisis estadístico.

- La información expuesta en las diferentes figuras gráficas representa casos que han trascendido públicamente; en ningún momento se reflejan datos de carácter personal.

Sobre Karont3

Vigila a quienes te vigilan, protege tu información

Breve introducción

Karont3 es un **observatorio de fugas de información** desarrollado por **Ewala** con la finalidad de detectar amenazas con alto impacto reputacional o económico; como herramienta **SaaS** te permite vigilar tu información crítica y medir tu riesgo ante la exposición de amenazas, así como tener visibilidad de todas tus búsquedas y hallazgos disponibles.

Con Karont3, vigilas a quienes te vigilan.

¿Cómo funciona?

Karont3 incorpora conexiones contra orígenes de datos externos, una base de datos propia gestionada íntegramente por el departamento de I+D+i de **Ewala**, en constante actualización, y un equipo humano de detección temprana de **Data Leak** en **Deep Web**, **Surface Web** y otros canales de distribución (WhatsApp, Telegram...).

Karont3 en Cifras

Datos incorporados en Karont3

Durante el año 2023 se han incorporado **46** nuevas colecciones de datos fugados, sumando una elevada cifra de colecciones (n > **460)** con miles de ficheros sensibles.

Las adquisiciones realizadas a lo largo del año 2023 han permitido operar con total independencia de las fuentes externas que complementan a **Karont3**, garantizando la auto-suficiencia como herramienta de **Threat Intelligence** y por tanto, la detección continua de datos críticos de nuestros clientes y partners.

El siguiente cuadro recoge las cifras de datos en bruto almacenadas en la base de datos de **Karont3** a fecha de **01/12/2023**.

Medios de obtención

El proceso de obtención de datos en bruto ha sido efectuado gracias a la vigilancia continua en **Dark Web** y **Surface Web**, así como también bajo la interacción con comunidades especializadas, siendo la **Surface Web** la principal zona de adquisición (Figura 1).

En lo que respecta al presente año, los medios principales de obtención de **Data Leaks** han sido foros especializados y, en menor medida, descargas directas mediante Torrent (Figura 2).

Figura 1. Análisis de orígenes de datos.

Figura 2. Canales de distribución.

Tendencia volumétrica

Los valores máximos de **Data Leaks** acumulados para el año 2023 pueden encontrarse en los meses de mayo (n=7.401 GB), seguido del mes de octubre (n=7152,7 GB) (Figura 3).

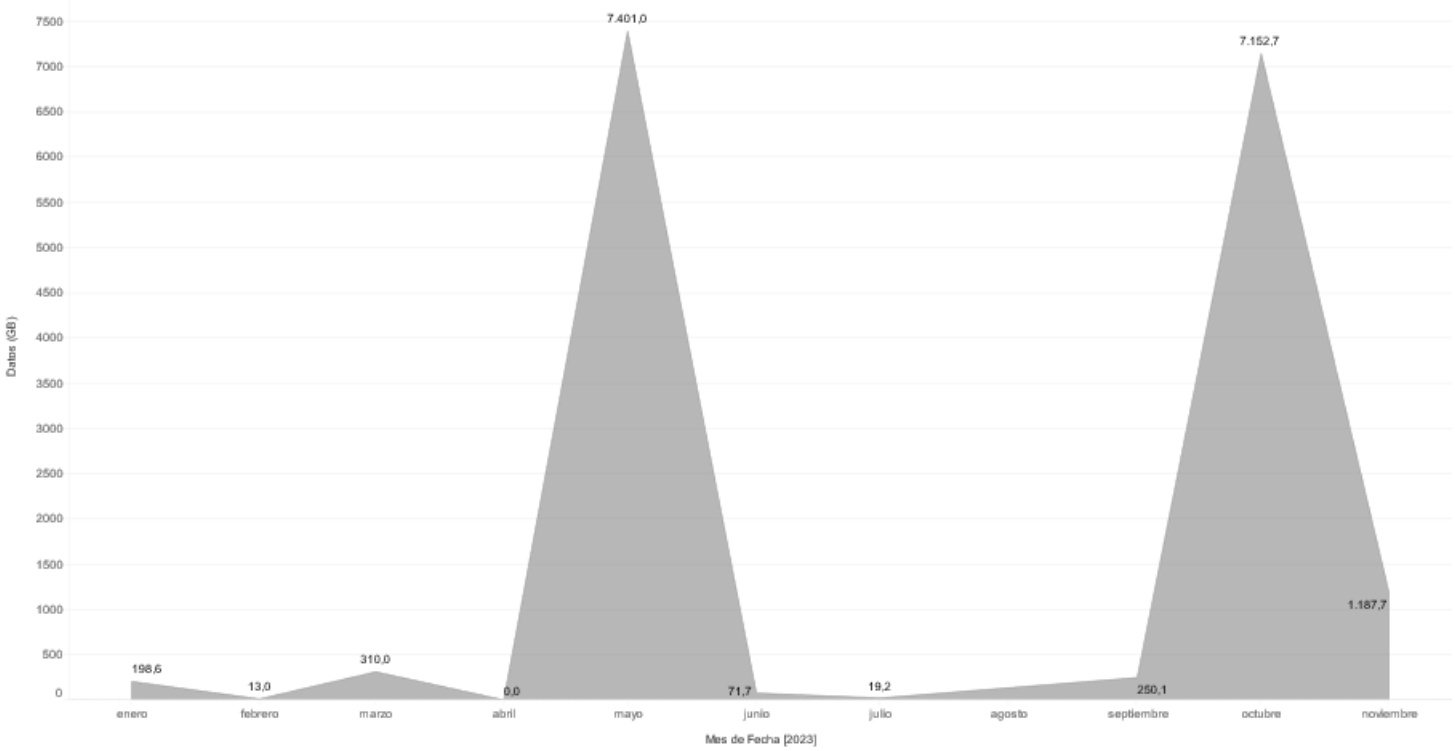


Figura 3. Tendencia volumétrica de datos fugados en 2023.

Sectores con mayor afectación

Por volumen de pérdidas

Desde una perspectiva de volumen de información fugada, o lo que es lo mismo, el peso total de los datos por cada ámbito sectorial, se detecta una mayor afectación en el sector **sanitario** (n=7.090 GB), seguido de **hospitales y farmacias y médicos** (n=4.700 GB) y **hardware** (n=1.510 GB) (Figura 4).

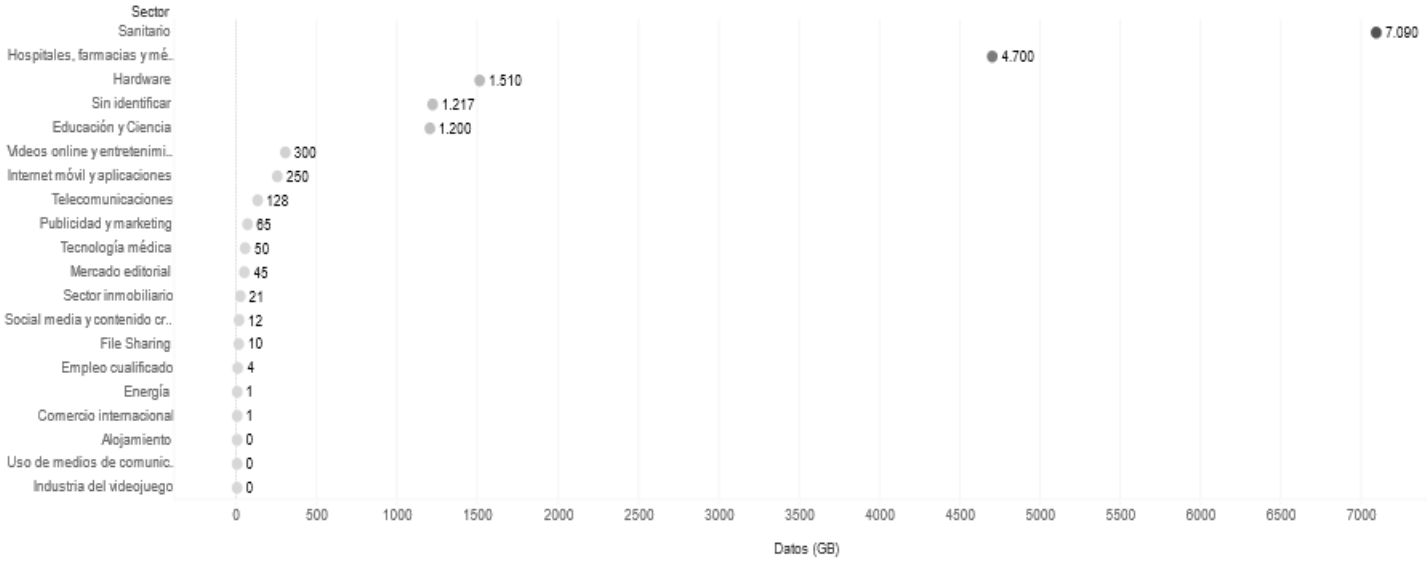


Figura 4. Volumen de data leaks por sectores en 2023.

En una vista agrupada, podemos distinguir con mayor claridad los sectores más impactados (véase Figura 5).

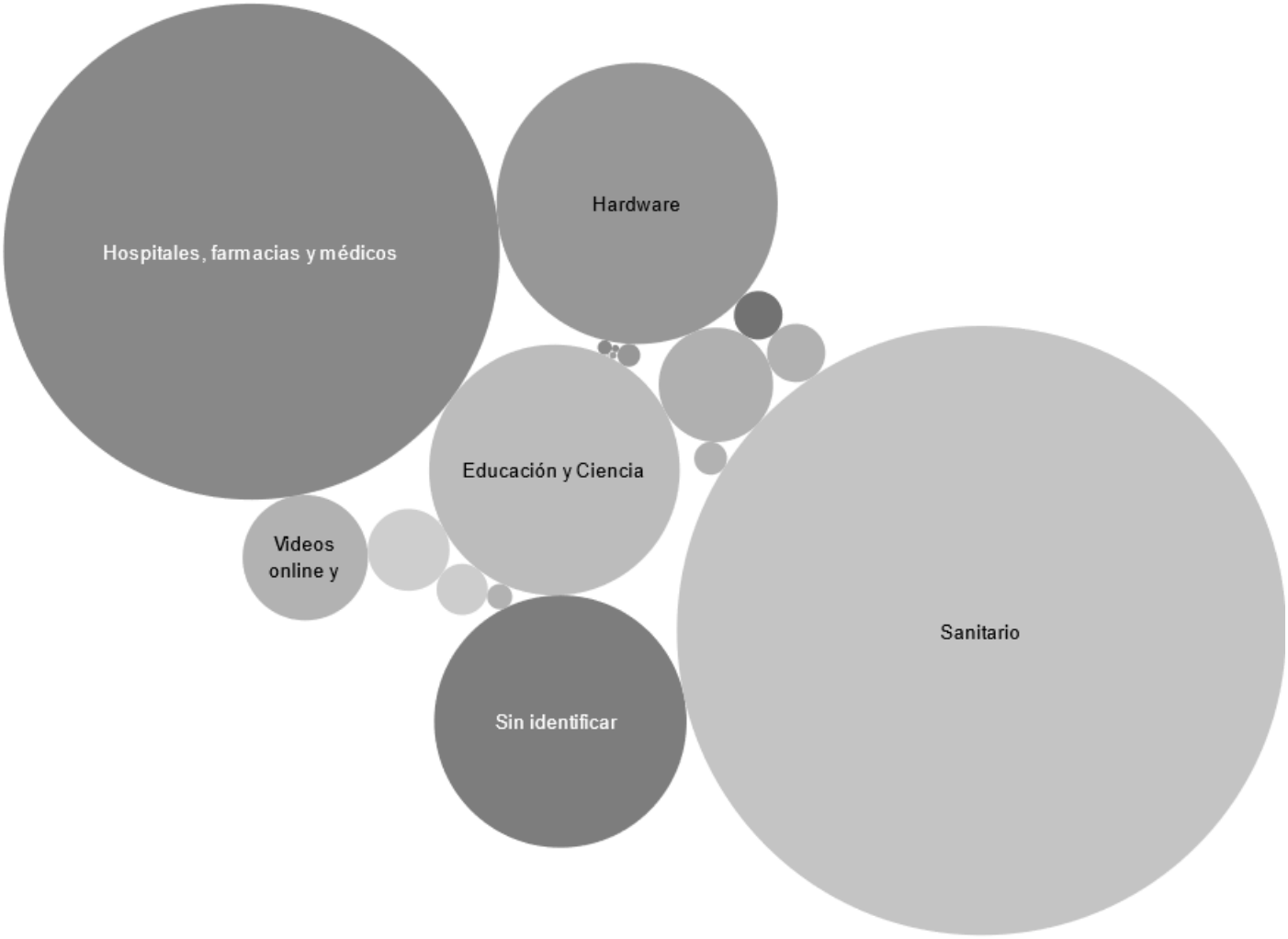


Figura 5. Distribución (volumétrica) de data leaks por sectores en 2023.

Por cantidad de fugas (colecciones)

En la siguiente figura se encuentran enumerados todos los sectores afectados y su relación con las colecciones almacenadas, dándonos la perspectiva de afectación sobre el número de veces que se han detectado fugas de información en un determinado sector.

Desde esta perspectiva, encabeza el ranking de sectores con mayor afectación las plataformas de **videos online**, seguido de plataformas de **social media**, y el sector **sanitario** (véase Figura 6).

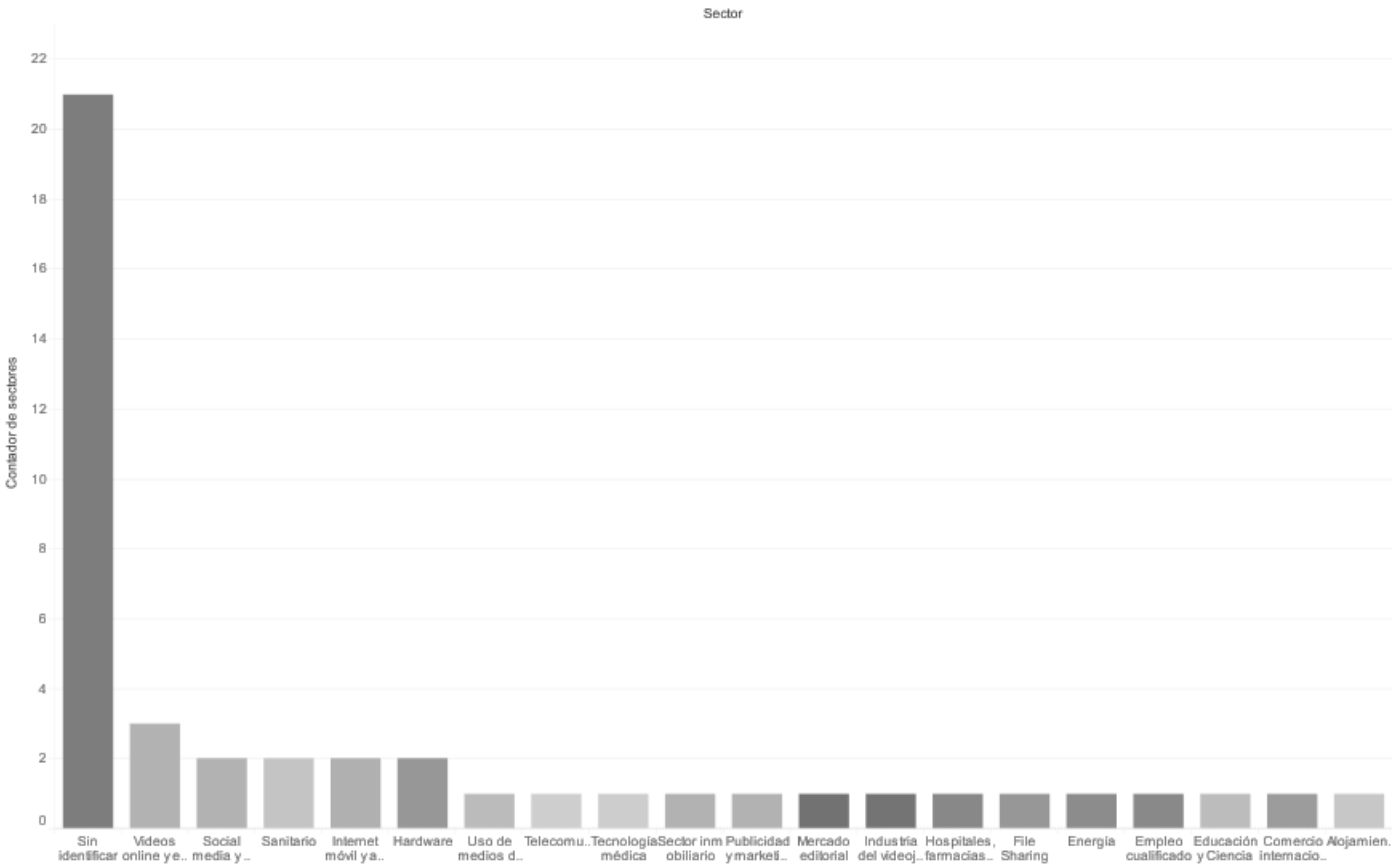


Figura 6. Cantidad de leaks por sectores en 2023.

Empresas con mayor volumen de datos fugados

En la siguiente gráfica podemos observar que las entidades con un mayor volumen de fugas de información han sido **Redcliffe Labs** y **PharMerica** (véase Figura 7).

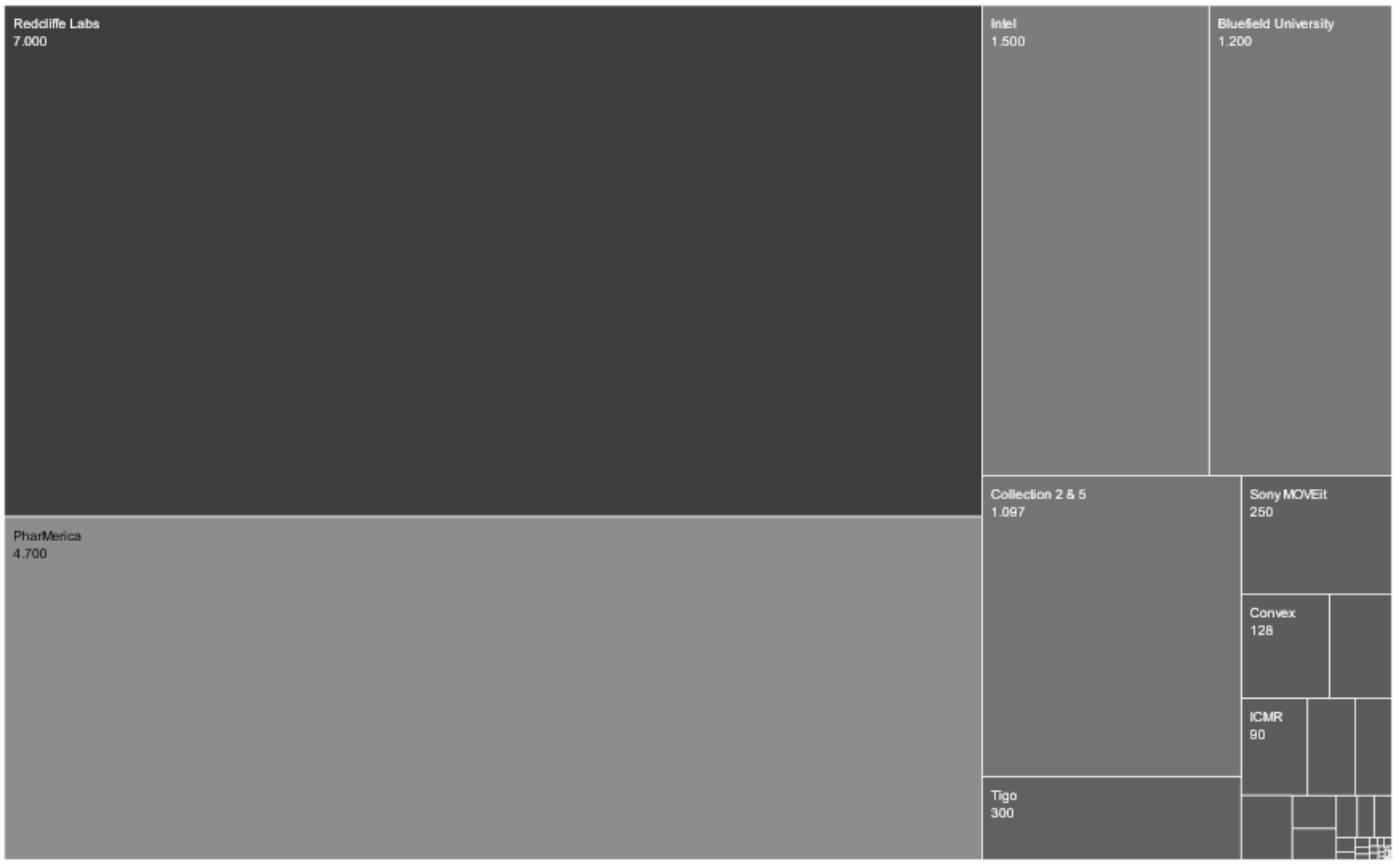


Figura 7. Empresas con mayor volumen de datos fugados.

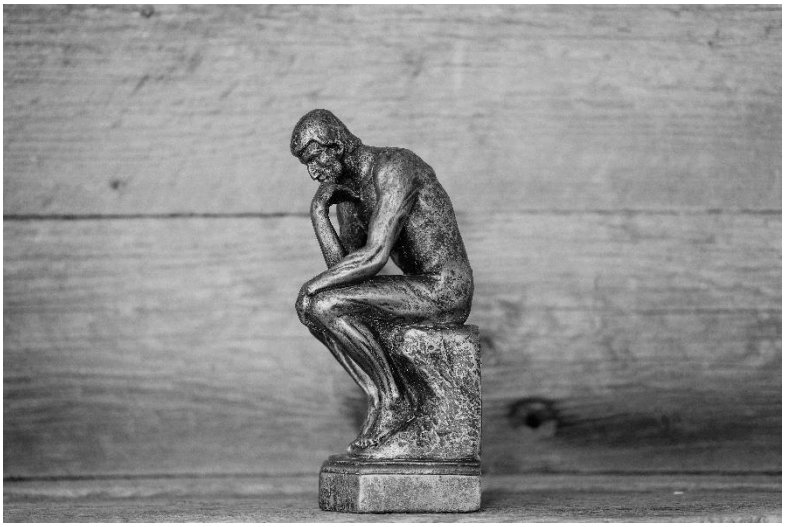
Distribución geográfica

Mediante el siguiente cartograma podemos observar la distribución espacial de los datos fugados durante el año 2023. Como puede observarse, el país con mayores fugas de información reportadas ha sido Estados Unidos de América; mención especial merece España, pues para el equipo de Karont3 resulta prioritario identificar y alertar a las empresas dentro de la geografía española (véase Figura 8).

Figura 8. Distribución geográfica de leaks detectados.

Conclusiones

El presente informe pretende, no solamente **concienciar ante una amenaza recurrente como es la fuga de información**, sino también proveer de datos objetivos al conjunto de profesionales del sector de la ciberseguridad y por extensión a todas las organizaciones que dependan de medidas lógicas de protección para un debido cuidado de sus datos críticos.



Como ha podido evidenciarse, el **Data Leak** afecta a empresas de diversos sectores, y es por ello que se recomienda contar con procedimientos que prevengan la fuga de datos, así como también mecanismos de detección temprana para aquella información que haya sido filtrada al público general.

¿Piensas en la fuga de datos? Pues no basta solo con pensar. ¡Llámanos!

Desde **Ewala** contamos con un equipo de investigadores en **Deep Web** y **Redes Sociales**, permitiéndonos estar al día de nuevos **Data Leaks**.

Si eres una organización pública o privada, y quieres estar al corriente de cualquier indicio de fuga de información que pueda afectar tu negocio, te invitamos a consultar más información sobre Karont3 mediante el siguiente enlace:

Más información

Si eres un usuario particular que se ha visto afectado por extorsión, te recomendamos llamar al número 017 perteneciente al **INCIBE**, en horario de 09:00 a 21:00 h.

ewala


CERTIFICADA
COMO EMPRESA
EMERGENTE
enisa
MINISTERIO
DE INDUSTRIA,
COMERCIO Y
TURISMO


PYME INNOVADORA
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN


CLUSTERTIC
Asturias


NODO
Seguridad de la Información de Asturias