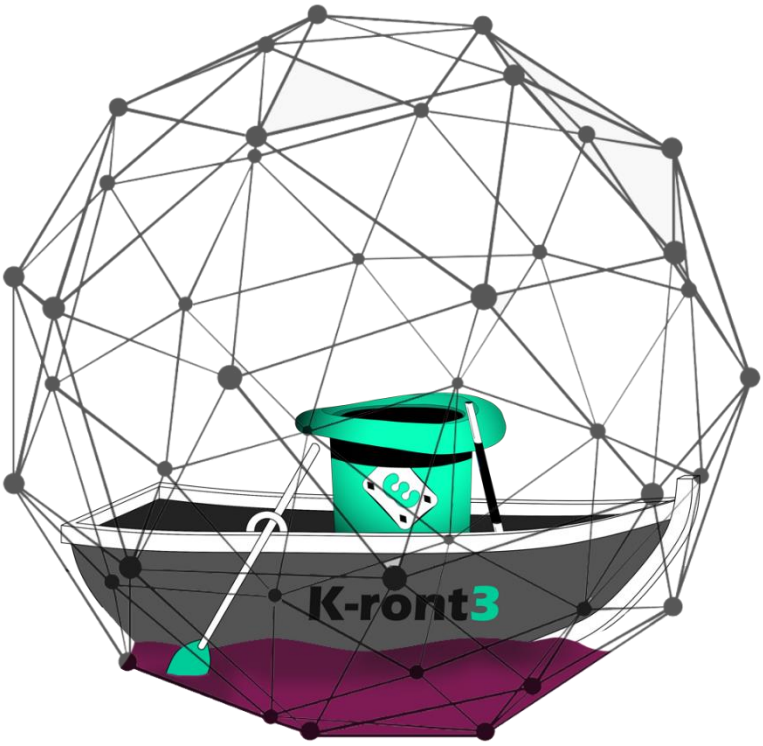
Ewala



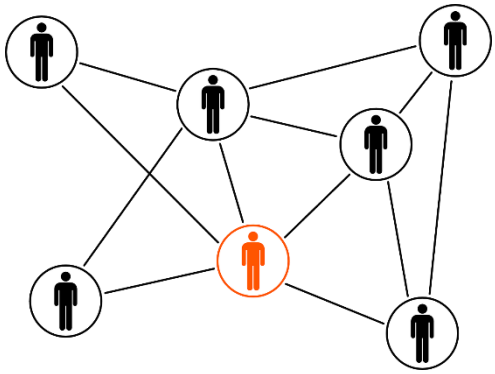
FUGA DE DATOS

Diciembre/2021

Tabla De Contenidos

Introducción

¿Qué son los Data leaks?



La **hiperconectividad** por parte de las empresas favorece la innovación tecnológica o 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 **abiertamente o en el mercado negro**.

A lo largo de los meses del presente año **2021** 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 canales de dudosa reputación. Un atacante vulnera el medio de envío no controlado y obtiene la información confidencial de la compañía.

Filtración Interna Mal-Intencionada

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 **K-ront3 Data Leak Observatory**, abarcando el intervalo de tiempo comprendido entre 01/2021 y 12/2021.

- 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.

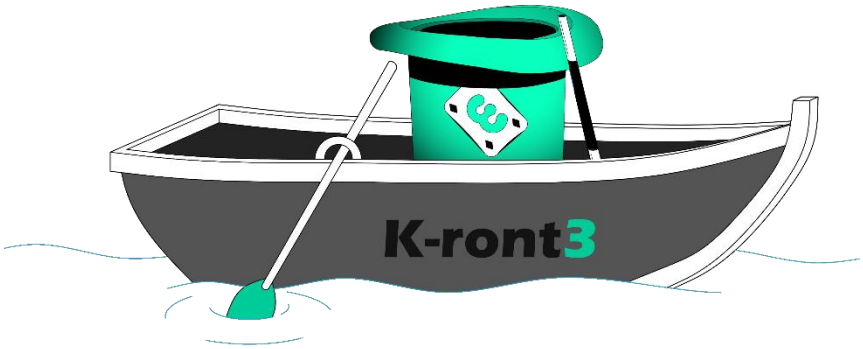
¿Qué es K-ront3?

Breve introducción

K-ront3 es una herramienta de **Threat Intelligence** desarrollada por **Ewala** que te permite detectar fugas de información con alto impacto reputacional o económico, brindándote la capacidad de medir tu riesgo ante la exposición de amenazas, así como tener visibilidad de todas tus búsquedas y hallazgos disponibles.

¿Cómo funciona?

K-ront3 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...).



K-ront3 en Cifras

Datos incorporados en K-ront3

Las adquisiciones realizadas a lo largo del año 2021 han permitido operar con total independencia de las fuentes externas que complementan a **K-ront3**, 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 **K-ront3** a fecha de **14/12/2021**.

Cantidad de colecciones (totales)	Cantidad de ficheros (totales)	Volumen (total) de ficheros	Cantidad de colecciones (2021)
274	304135	>1TB	65

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.

En lo que respecta al presente año, los medios principales de obtención de **Data Leaks** han sido las redes sociales y torrents (**Surface Web**), seguido por portales distribuidos en la **Dark Web** y otras vías de acceso mediante pago (Figura 1).

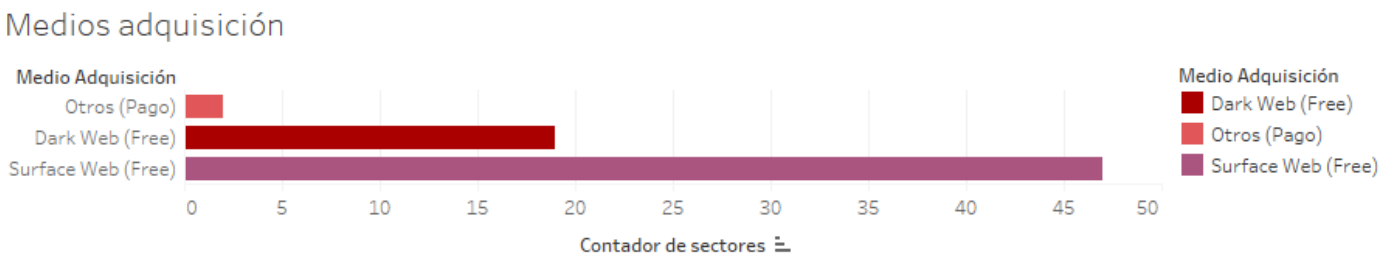


Figura 1. Análisis de orígenes de datos.

Tendencia volumétrica

Los valores máximos de **Data Leaks** acumulados para el año 2021 pueden encontrarse en los meses de enero (n=470), abril (n=222,6), julio (n=756,4 Gb), y octubre (n=140,3 GB), detectándose fugas de información elevadas cada 3 meses (véase Figura 2).

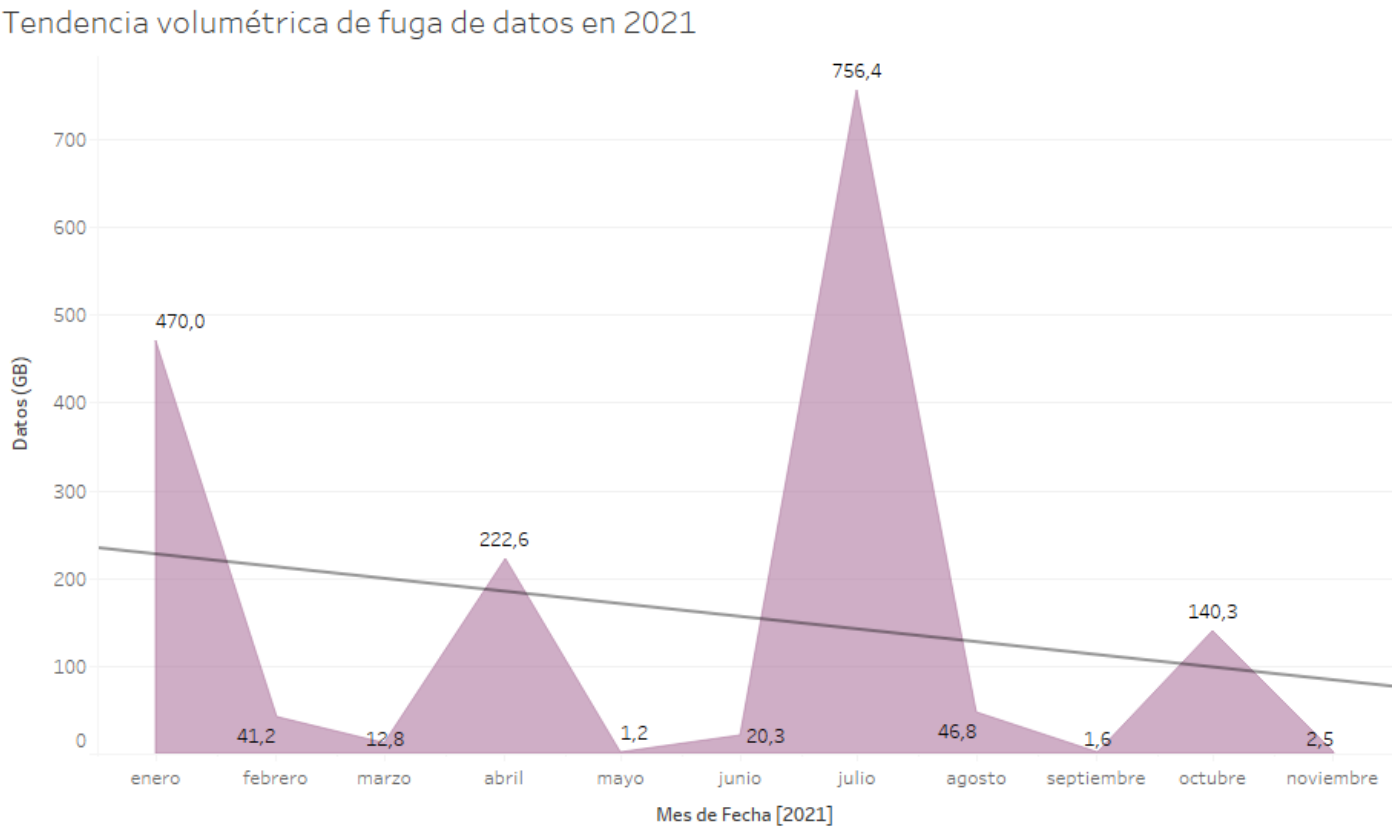


Figura 2. Tendencial volumétrica de datos fugados en 2021.

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 empresarial, se detecta una mayor afectación en **la industria del videojuego, las redes sociales y la industria de videos online y entretenimiento, seguido de las industrias de telecomunicaciones, ropa y complemento** (véase Figura 3).

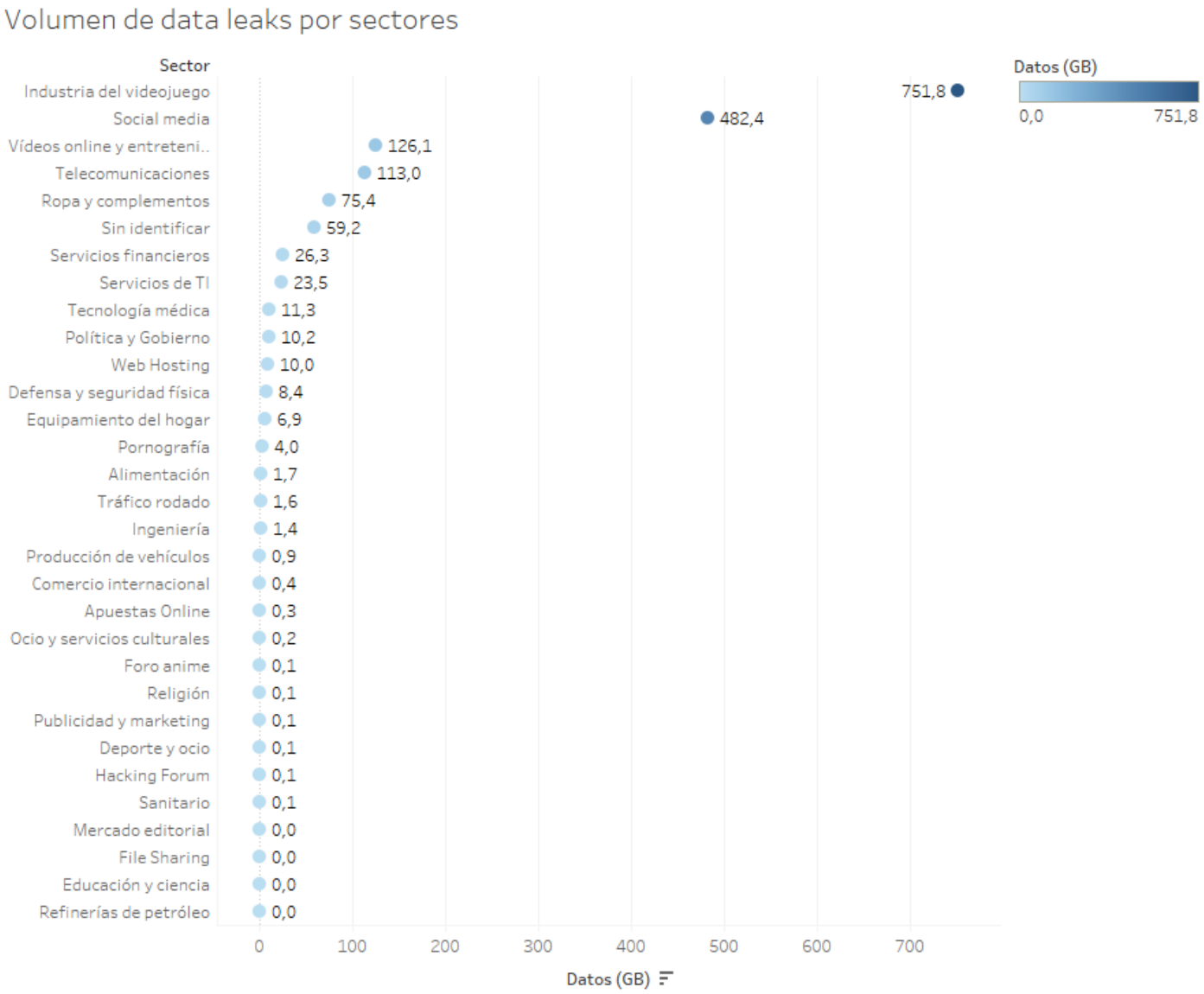


Figura 3. Volumen de data leaks por sectores en 2021.

En una vista agrupada, podemos distinguir con mayor claridad los sectores más impactados (véase Figura 4).

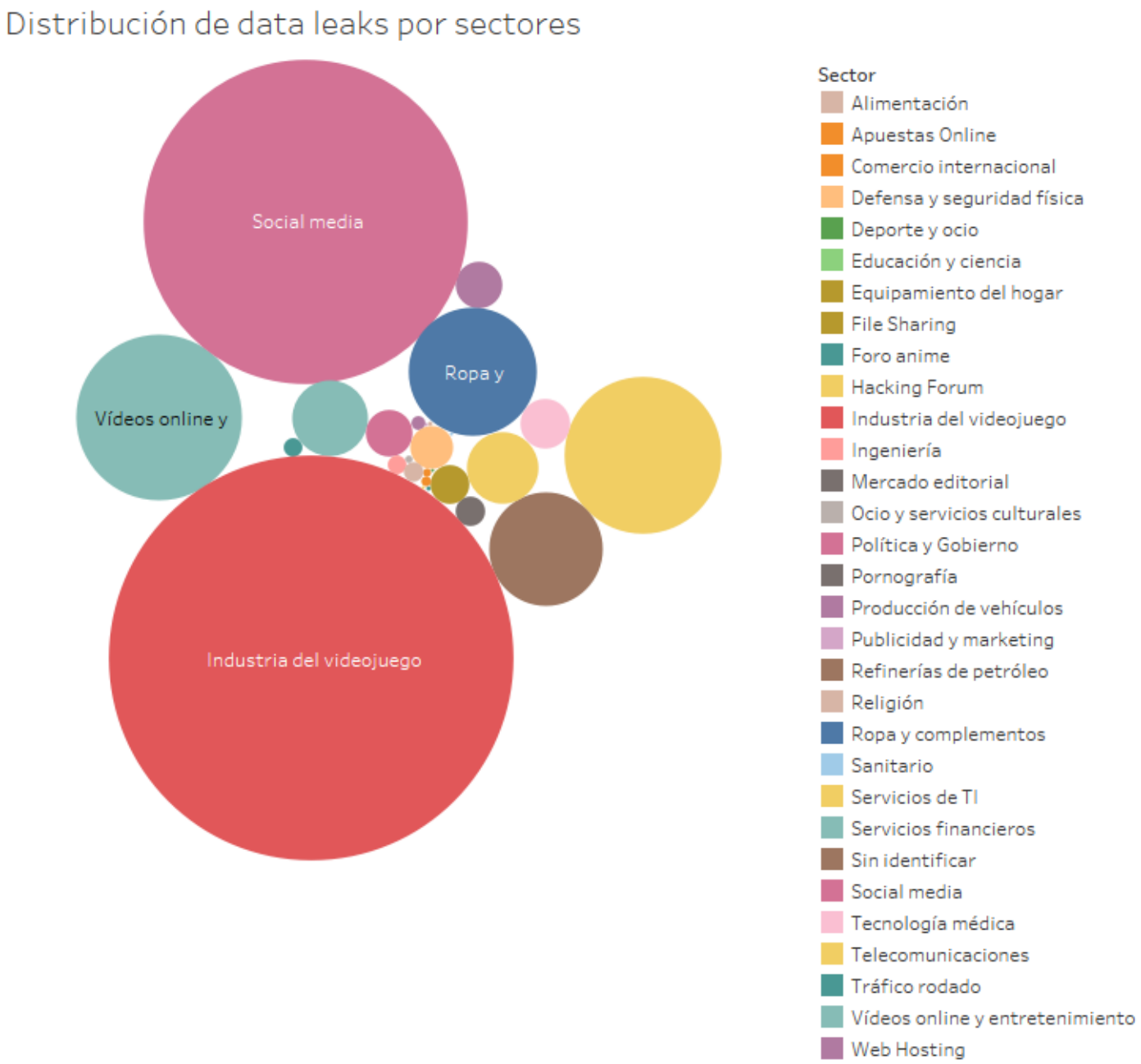


Figura 4. Distribución (volumétrica) de data leaks por sectores en 2021.

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, vuelve a encabezar el ránking de sectores con mayor afectación la industria de **videos online y entretenimiento, seguido de las redes sociales e industria del videojuego** (véase Figura 5).

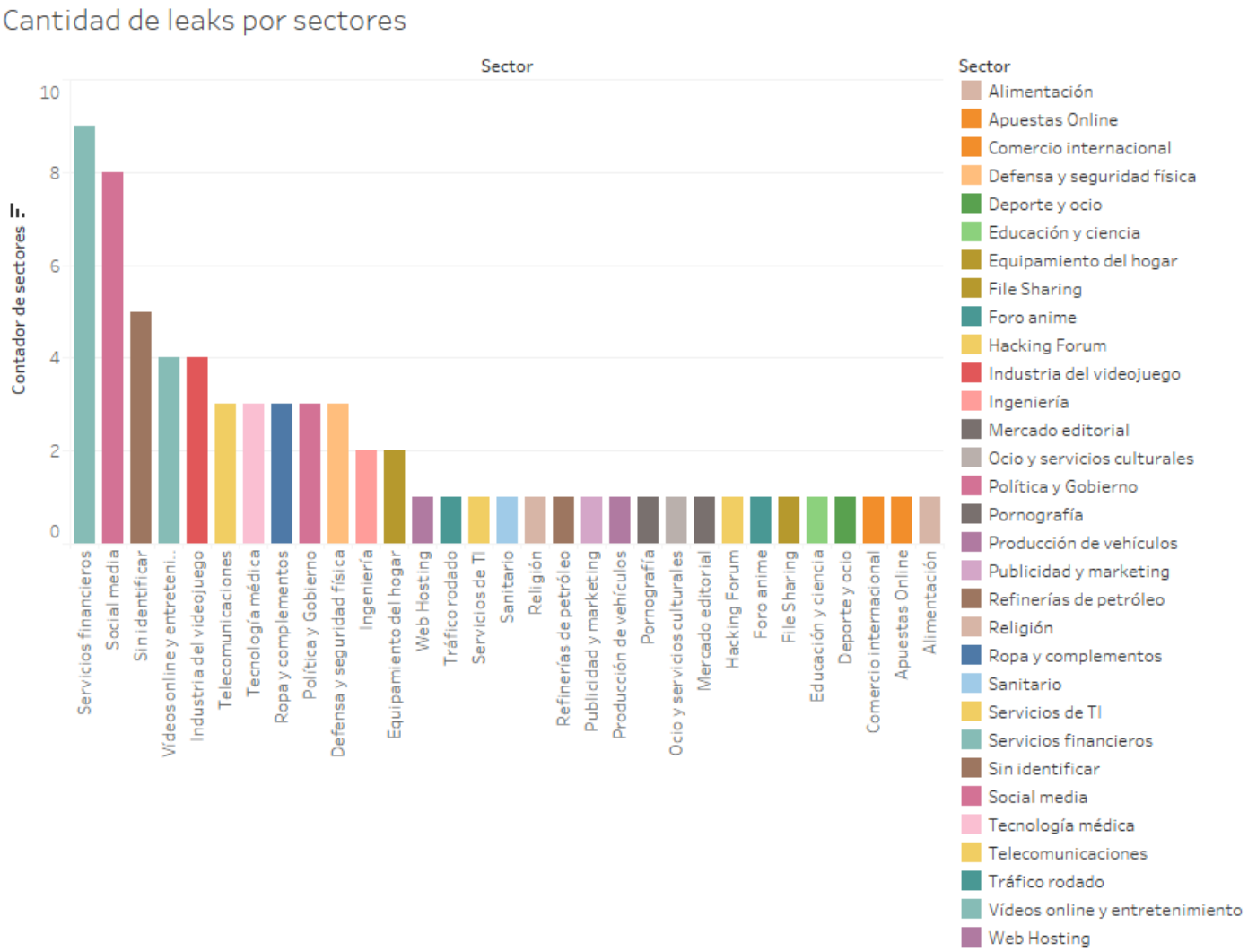


Figura 5. Cantidad de leaks por sectores en 2021.

Empresas con mayor volumen de datos fugados

En la siguiente gráfica podemos observar que las cinco empresas con un mayor volumen de fugas de información han sido **EA Games, Sociallarks, Twitch, y Phonehouse, y Facebook** (véase Figura 6).

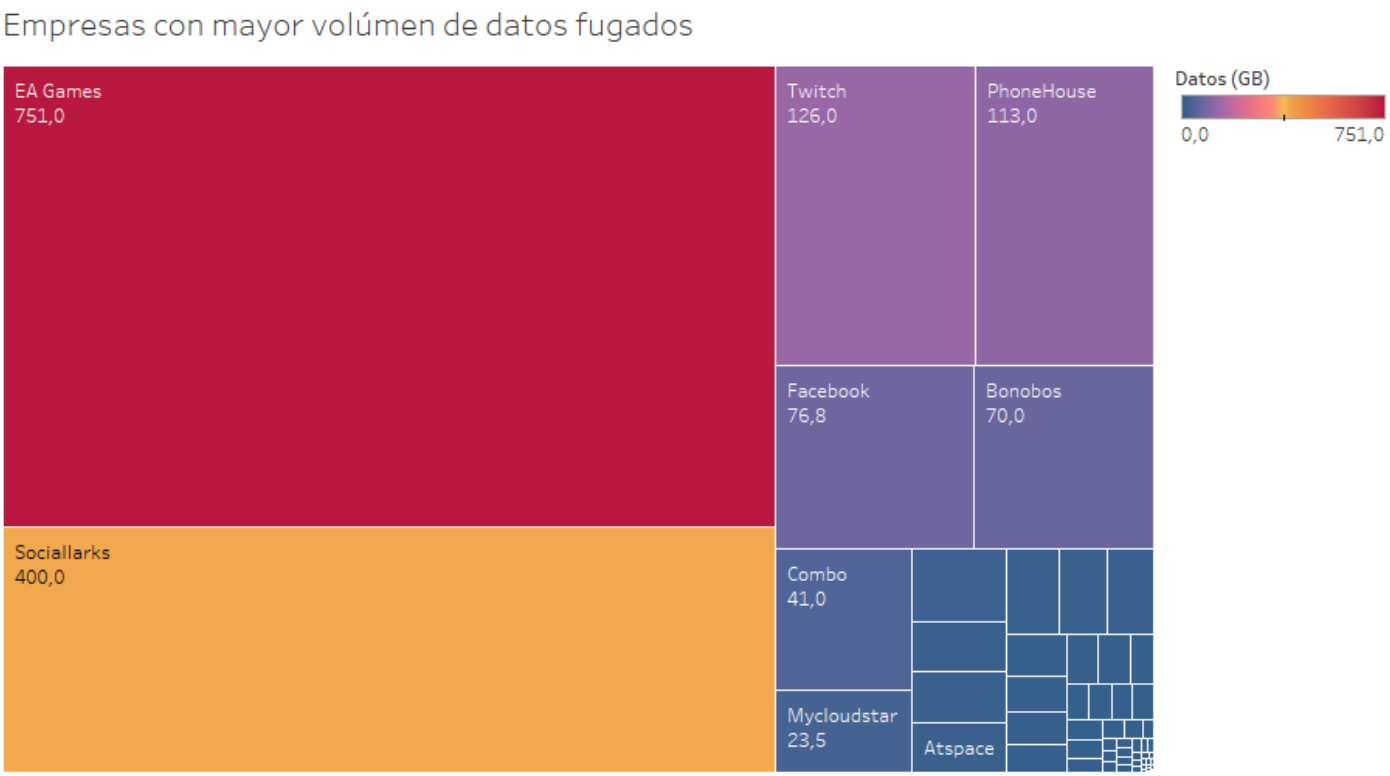


Figura 6. Empresas con mayor volumen de datos fugados.

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.

Ewala! | Security Wizards
www.ewala.es

Desde **Ewala IT Services** 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 K-ront3 mediante el siguiente enlace:

Kront3.ewala.es

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.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

Para conocer más acerca de K-ront3 Data Leak Observatory visita: kront3.ewala.es

Para conocer más acerca de Ewala IT Services, visita:

Página web Ewala

Perfil de Linkedin

Canal de Youtube

Ewala IT Services

Residencia empresarial EnPrendes, (Prendes), Carreño.
info@ewala.es

Sobre K-ront3

K-ront3 es una aplicación que te permite localizar a tiempo la información confidencial de tu empresa que se encuentra bajo dominio público o en el mercado negro.

Sobre Ewala IT Services

Ewala es una empresa de ciberseguridad: desarrollamos productos propios y ofrecemos consultoría, tanto IT como OT.