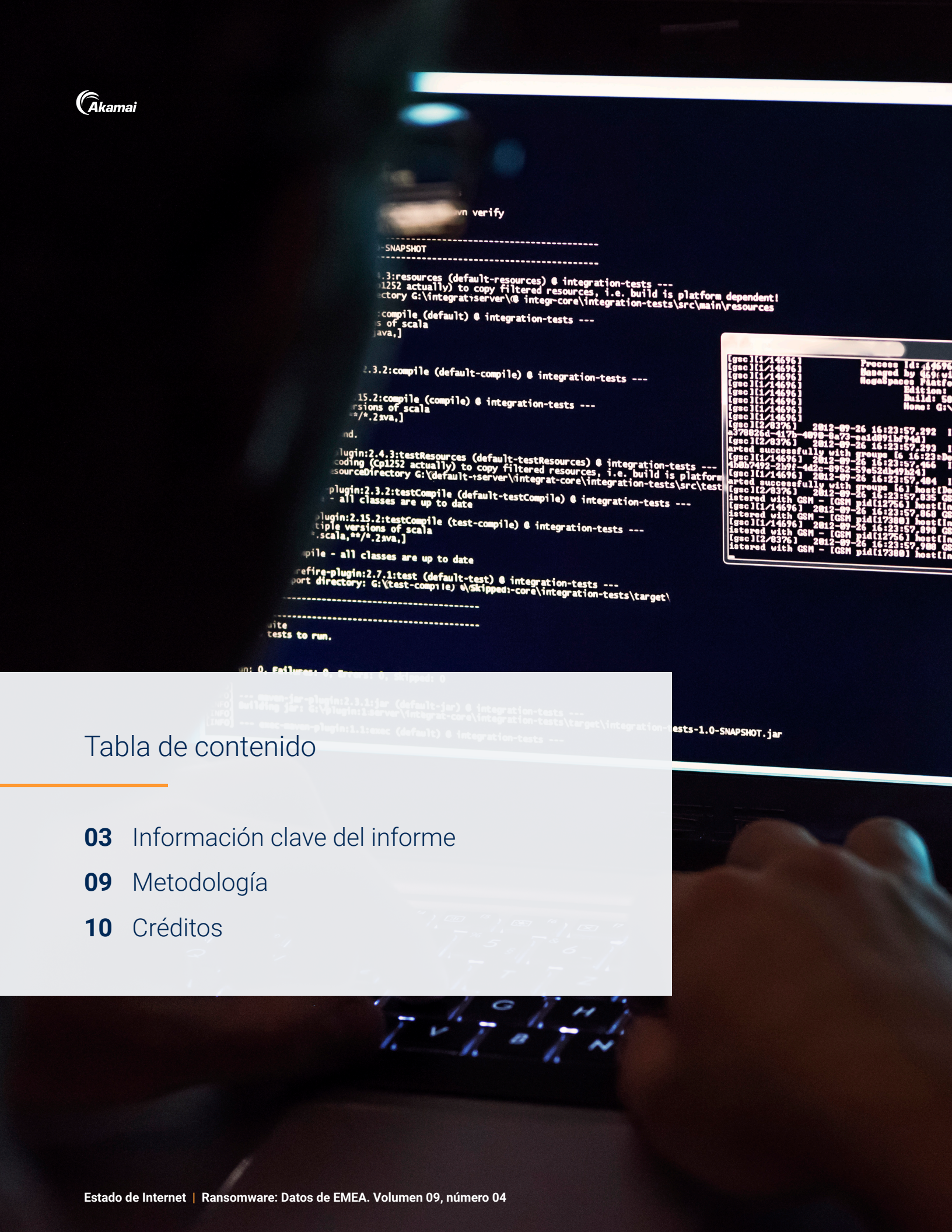
Akamai

Estado de Internet
Volumen 09 | Número 04

# El ransomware en movimiento

Datos de EMEA



# Tabla de contenido


**03** Información clave del informe

**09** Metodología

**10** Créditos

# Información clave del informe

Datos de EMEA es un documento complementario a nuestro informe sobre el estado de Internet en materia de seguridad (SOTI) de ransomware, más detallado, El ransomware en movimiento: evolución de las técnicas de explotación y la búsqueda activa de día cero (disponible solo en inglés). En este informe podrá consultar análisis detallados de las tendencias, la metodología y las técnicas de ataque de los grupos de ransomware, una descripción de las fases de los ataques, así como las soluciones y recomendaciones correspondientes para proteger su organización, además de nuestras metodologías de investigación.

## Descripción general

El ransomware sigue causando estragos en las empresas y cobrándose más víctimas a medida que los adversarios siguen evolucionando y cambiando sus técnicas de ataque, introduciendo así nuevos métodos de extorsión, aprovechando una superficie de ataque en expansión y sacando partido a las restricciones presupuestarias en materia de seguridad. El impacto de estas peligrosas tendencias se refleja en los grupos de ransomware que dominan el panorama y en su creciente éxito. En EMEA, esto se ejemplifica con un crecimiento del 18 % en las empresas víctimas entre el cuarto trimestre de 2021 y el cuarto trimestre de 2022, y con un aumento del 77 % en el recuento de víctimas interanual si se compara el primer trimestre de 2022 con el primer trimestre de 2023.

En este Datos de EMEA compartimos información adicional para mejorar la defensa y la gestión de riesgos de esta preocupación cada vez mayor, como los siguientes datos:

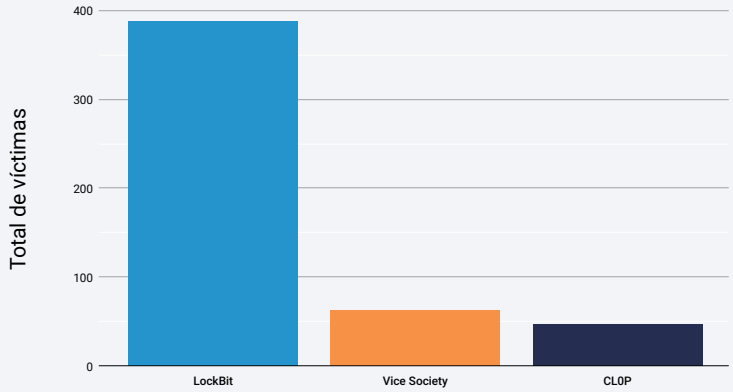
- Entre octubre de 2021 y mayo de 2023, LockBit controló el panorama del ransomware, junto con el aumento de CL0P, que aprovechaba agresivamente las vulnerabilidades. Un cambio en las técnicas de ataque, del phishing al creciente abuso de las vulnerabilidades de día cero y de primer día, desembocó en un brusco aumento de víctimas.
- De acuerdo con los hallazgos a nivel mundial, la fabricación fue el sector con el mayor número de organizaciones víctimas, seguido de los servicios empresariales.
- La mayoría de las víctimas de ransomware eran organizaciones más pequeñas con unos ingresos de hasta 50 millones de USD. Sin embargo, las organizaciones más grandes también fueron objeto de ataques.

## LockBit domina la actividad de los grupos de ransomware

A pesar de la creciente concienciación sobre el ransomware y de la gran cantidad de herramientas y prácticas recomendadas disponibles para combatir esta amenaza, el incremento de las empresas víctimas en la región de EMEA fue de un 18 % entre el cuarto trimestre de 2021 y el cuarto trimestre de 2022, con un aumento del 77 % en el recuento de víctimas interanual si se compara el primer trimestre de 2022 con el primer trimestre de 2023. De acuerdo con los datos obtenidos en nuestro informe global, en el periodo comprendido entre el 1 de octubre de 2021 y el 31 de mayo de 2023, LockBit fue responsable de la mayoría de los ataques, con un 45 % de los ataques en EMEA. Sin embargo, en la región EMEA, Vice Society sustituye a ALPHV como segundo grupo más activo; CL0P sigue ocupando la tercera posición (EMEA - Figura 1).

**EMEA: 3 grupos de ransomware principales por recuento de víctimas**

Del 1 de octubre de 2021 al 31 de mayo de 2023




*EMEA - Fig. 1: La mayoría de las organizaciones víctimas de ataques de ransomware en EMEA sufrieron los ataques de LockBit, Vice Society y CL0P*

## Análisis trimestral

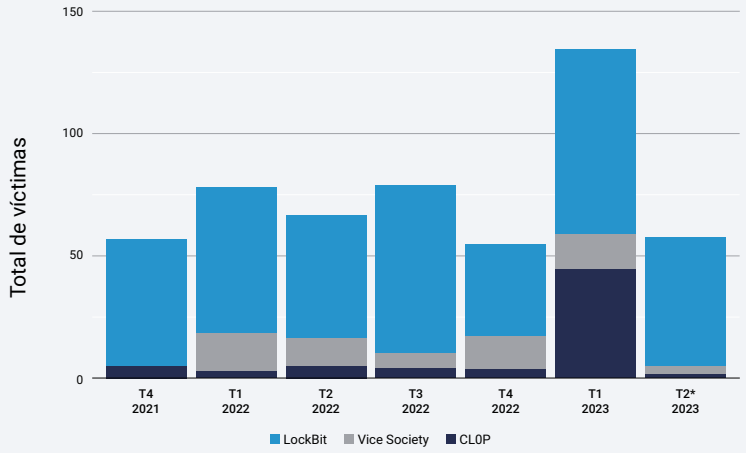
Si observamos el número de víctimas por grupo de ransomware (EMEA - Figura 2), LockBit sigue siendo prevalente, mientras que la presencia continua de Vice Society probablemente vaya de la mano con el hecho de que el sector de la educación es uno de los principales objetivos de los ataques de ransomware en EMEA (como se muestra más adelante en la figura 3), ya que Vice Society es una oferta de ransomware como servicio cuyo objetivo claro es el sector educativo. Sin embargo, de acuerdo con las tendencias de datos globales, CL0P está aumentando en el panorama del ransomware de EMEA. Su pico en el primer trimestre de 2023 puede atribuirse a su explotación de diversas vulnerabilidades

** T2 2023 no es un trimestre completo, ya que los datos son hasta el 31 de mayo de 2023.*

de día cero como punto de entrada. Un cambio en las técnicas de ataque durante los últimos seis meses, del phishing al abuso cada vez mayor de las vulnerabilidades, está desembocando en el brusco aumento de víctimas. Dicho esto, solo se disponía de datos parciales para el segundo trimestre de 2023* en el momento de redactarse el presente informe. A partir del 31 de mayo de 2023, la actividad de CL0P volvió al nivel que observamos en 2022. Aunque no podemos afirmar con seguridad lo que deparará el trimestre, es importante tener en cuenta que en junio de 2023 CL0P publicó los nombres de más empresas víctimas en EMEA como consecuencia de la explotación de la vulnerabilidad de MOVEit, por lo que es muy posible que el número de afectados aumente.

**EMEA: 3 grupos de ransomware principales por recuento de víctimas**

Trimestral: Del 1 de octubre de 2021 al 31 de mayo de 2023




*EMEA - Fig. 2: Comparación trimestral del número de víctimas entre los tres grupos principales de ransomware de EMEA: LockBit, Vice Society y CL0P*

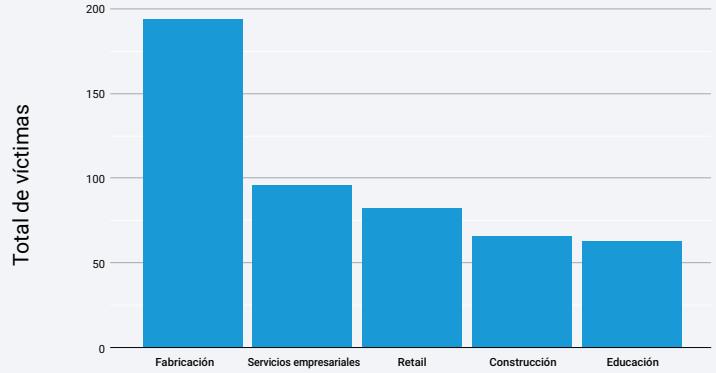
## Sectores principales en riesgo

Los cinco sectores principales en riesgo de sufrir un ataque de ransomware en EMEA son fabricación, servicios empresariales, retail, construcción y educación (EMEA - Figura 3). Estos datos se corresponden con los mismos cinco sectores principales a nivel mundial y también son coherentes con el informe global de ransomware de 2022, en el que la fabricación y los servicios empresariales ocuparon las dos primeras posiciones. Durante ese tiempo, recibieron ataques del ransomware Conti. Tras desaparecer Conti, LockBit ocupó el lugar dejado vacante. También observamos una importante superposición con los cinco sectores más afectados en nuestro informe de DNS anterior, Superautopista de ataques: profundizamos en el tráfico de DNS malicioso, que refleja una evidente relación entre el tráfico malicioso de mando y control (C2) y los ataques de ransomware.

** T2 2023 no es un trimestre completo, ya que los datos son hasta el 31 de mayo de 2023.*

**EMEA: Los 5 principales sectores según el volumen de víctimas de grupos de ransomware**

Del 1 de octubre de 2021 al 31 de mayo de 2023




*EMEA - Fig. 3: La fabricación es el sector con el mayor número de empresas víctimas de ataques de ransomware en EMEA.*

También es importante tener en cuenta que LockBit es el ransomware más frecuente en cada uno de los cuatro sectores principales de EMEA, con un 45,9 % de los ataques en el sector de fabricación, un 45,4 % en servicios empresariales, un 45,1 % en retail y un 53,6 % en la construcción. El sector de la educación es la excepción: Vice Society está detrás del mayor número de ataques (36,5 %), mientras que LockBit registra el 22,2 % de los mismos.

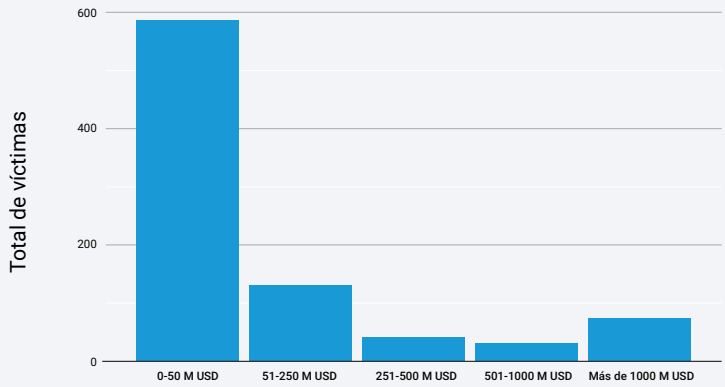
> Todas las empresas, independientemente de cuál sea su tamaño o sus ingresos, corren el riesgo de sufrir ataques de ransomware.

## Los grupos de ransomware se centran en el retorno de la inversión

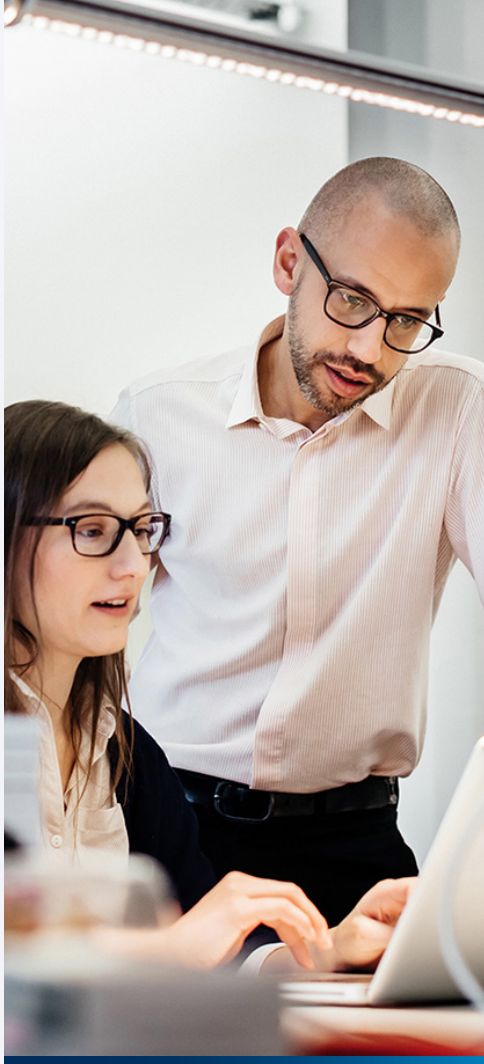
Todas las empresas, independientemente de cuál sea su tamaño o sus ingresos, corren el riesgo de sufrir ataques de ransomware. Sin embargo, conforme a la tendencia mundial, los datos muestran que los atacantes consiguen lanzar ataques contra empresas más pequeñas en la región EMEA (EMEA - Figura 4). Suponemos que las empresas más pequeñas tienen recursos de seguridad limitados a la hora de luchar contra el ransomware, por lo que resultan más vulnerables y es más fácil infiltrarse en ellas y que pueden pagar el rescate. Sin embargo, las empresas más grandes también son objeto de ataques. Las investigaciones muestran que cuanto mayores son los ingresos de la organización afectada, mayor es el importe del rescate.

**EMEA: Víctimas totales por rango de ingresos del grupo de ransomware**

Del 1 de octubre de 2021 al 31 de mayo de 2023




*EMEA - Fig. 4: La mayoría de víctimas de ransomware en EMEA se encuentran en organizaciones con unos ingresos de hasta 50 millones de USD.*



## Conclusión de Datos de EMEA

El ransomware sigue causando estragos en las empresas. A nivel mundial y regional, los gobiernos están creando un frente unido para hacer frente a la amenaza, además de destacar técnicas que puedan ayudar a los encargados de la seguridad a proteger sus organizaciones y a aumentar la capacidad de resistencia. ENISA, la Agencia de la Unión Europea para la Ciberseguridad, ha emitido una nueva directiva relativa a la seguridad de las redes y sistemas de información (NIS2), diseñada para mejorar la ciberseguridad en toda la UE, y que incluye nuevas tareas como la creación de un registro de vulnerabilidades. Fuera del marco de la UE, otros países también están creando y aplicando sus propios controles, como la Autoridad Nacional de Ciberseguridad de Arabia Saudí (NCA).

A medida que los reguladores ponen en práctica iniciativas y políticas para reforzar los estándares en materia de ciberseguridad, es importante que sepa cuáles son los requisitos de presentación de informes en su área para que pueda incluirlos en su guía o plan de gestión de crisis y, de esta forma, ser consciente de las oportunidades que tiene de mitigar el riesgo mediante una defensa multicapa.

**Para obtener más información, consulte el informe SOTI global de ransomware, El ransomware en movimiento: evolución de las técnicas de explotación y la búsqueda activa de día cero.**

# Metodología

## Datos de ransomware

Los datos de ransomware utilizados en este informe se recopilaron de los sitios de filtración de aproximadamente 90 grupos de ransomware diferentes. Es típico de estos grupos dar detalles de sus ataques, como la hora del evento, los nombres de las víctimas y sus dominios. Es importante tener en cuenta que estos informes dependen de lo que cada grupo de ransomware desee publicar. No se ha incluido el éxito de estos ataques notificados en esta investigación.

En su lugar, el informe se ha centrado en las víctimas. Para cada análisis se midió el número de víctimas únicas dentro de cada grupo. Estos datos se unieron a los datos obtenidos de ZoomInfo para proporcionar detalles adicionales sobre cada víctima, como la ubicación, el rango de ingresos y el sector.

Todos los datos recogidos pertenecen al periodo de 20 meses comprendido entre el 1 de octubre de 2021 y el 31 de mayo de 2023.

## Créditos

### Editorial y redacción

Ori David
Badette Tribbey
Charlotte Pelliccia
Lance Rhodes

### Revisión y expertos en la materia

Moshe Cohen
Shiran Guez
Ophir Harpaz
Reuben Koh
Richard Meeus
Steve Winterfeld
Maxim Zavodchik

### Análisis de datos

Chelsea Tuttle

### Marketing y publicación

Kimberly Gomez
Georgina Morales Hampe
Shivangi Sahu

## Más información acerca de Estado de Internet/Seguridad

Lea números anteriores del aclamado informe sobre el estado de Internet en materia de seguridad de Akamai y entérese de cuándo se publican los siguientes números.
**akamai.com/soti**

## Más información acerca de la investigación de Akamai sobre amenazas

Conozca los últimos análisis de inteligencia frente a amenazas, informes de seguridad e investigación sobre ciberseguridad.
**akamai.com/security-research**

## Datos de Akamai de este informe

Vea versiones de alta calidad de los gráficos a los que se hace referencia en este informe. Puede usar estas imágenes y hacer referencia a ellas libremente, siempre que se cite debidamente a Akamai como fuente y que se conserve el logotipo de Akamai. **akamai.com/sotidata**

## Más información sobre las soluciones de Akamai

Si desea obtener más información sobre las soluciones de Akamai para combatir el ransomware, visite nuestra página de **soluciones de seguridad**.

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Akamai Connected Cloud, una plataforma de Edge y en la nube de distribución masiva, acerca las aplicaciones y las experiencias a los usuarios y aleja las amenazas. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado el 23 de agosto.