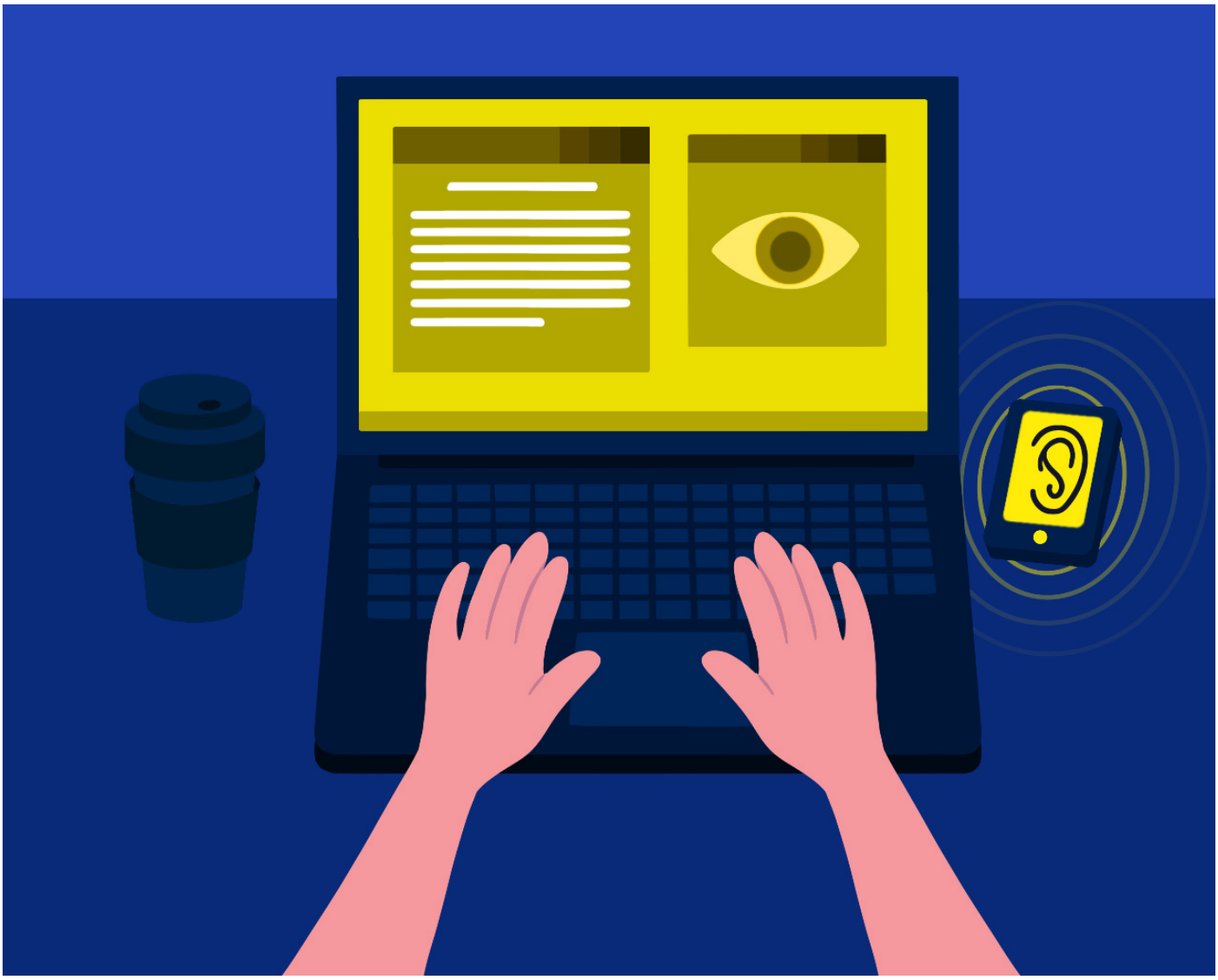


El estado del **stalkerware** en 2021

COALITION AGAINST STALKERWARE

kaspersky

Contenido

Principales descubrimientos de 2021

Cada año, Kaspersky analiza el uso de stalkerware por todo el mundo para comprender mejor la amenaza que supone. Nos asociamos con partes interesadas de los sectores público y privado para concienciar y buscar las soluciones que mejor nos permitan hacer frente a este importante problema.

El stalkerware permite espiar en secreto la vida privada de otras personas a través de dispositivos inteligentes. Suele utilizarse para ejercer violencia psicológica y física contra la pareja. El software está disponible de forma comercial y puede acceder a datos personales como la ubicación del dispositivo, el historial de navegación, mensajes de texto, chats de redes sociales, fotos y mucho más. Comercializar stalkerware no es ilegal, pero usarlo sin el consentimiento de la víctima sí lo es. Los perpetradores aprovechan este impreciso marco legal que todavía existe en muchos países. El stalkerware es una violación de la privacidad y una forma de abuso de la tecnología. Para hacer frente a esta compleja amenaza de una forma completa que apoye a víctimas y supervivientes, es necesario contar con herramientas desde el punto de vista legislativo, social y tecnológico.

Aspectos destacados de los datos en 2021

- **Los datos de Kaspersky muestran que, en 2021, 32 694 usuarios únicos se vieron afectados por stalkerware en todo el mundo.** Se trata de una cifra menor a la registrada en 2020 y la más baja desde que empezamos a recopilar datos sobre stalkerware en 2018. Y aunque podría ser un motivo de celebración, no lo es.
- **La ciberviolencia va en aumento,** sobre todo desde el inicio de la pandemia. Las personas han empezado a socializar menos y a pasar más tiempo en casa, por lo que los agresores sienten que tienen un mayor control y son menos propensos a instalar stalkerware para espiar a su pareja. Lamentablemente, disponen además de un mayor número de medios, como dispositivos inteligentes, para espiar o acechar sus víctimas. Las organizaciones sin ánimo de lucro con las que Kaspersky colabora estrechamente han compartido observaciones similares tras trabajar con agresores y víctimas de stalkerware. Es importante recordar que estas cifras solo incluyen a usuarios de Kaspersky y no tienen en cuenta a los usuarios que utilizan soluciones de seguridad de TI de la competencia o a aquellos que no tienen ninguna solución de seguridad TI instalada en sus móviles. Por lo tanto, solo vemos la punta del iceberg: aunque resulta difícil calcular el número exacto de usuarios afectados en el mundo, los miembros de la Coalition against Stalkerware calculan que el número podría ser al menos 30 veces mayor, con cerca de un millón de víctimas en todo el mundo, cada año.

- Según los datos obtenidos de Kaspersky Security Network, **los países más afectados siguen siendo Rusia, Brasil y Estados Unidos,** lo que coincide con las estadísticas de los últimos dos años. A nivel regional, hemos observado que el mayor número de usuarios afectados se encuentra en:
  - Alemania, Italia y el Reino Unido (Europa)
  - Turquía, Egipto y Arabia Saudí (Oriente Medio y África)
  - India, Indonesia y Vietnam (Asia Pacífico)
  - Brasil, México y Colombia (Latinoamérica)
  - Estados Unidos (Norteamérica)
  - La Federación Rusa, Ucrania y Kazajistán (Europa del Este — excluyendo países de la UE —, Rusia y Asia Central)
- **Cerberus y Reptilicus son las aplicaciones de stalkerware más utilizadas**, con 5575 y 4417 usuarios afectados, respectivamente, en todo el mundo.

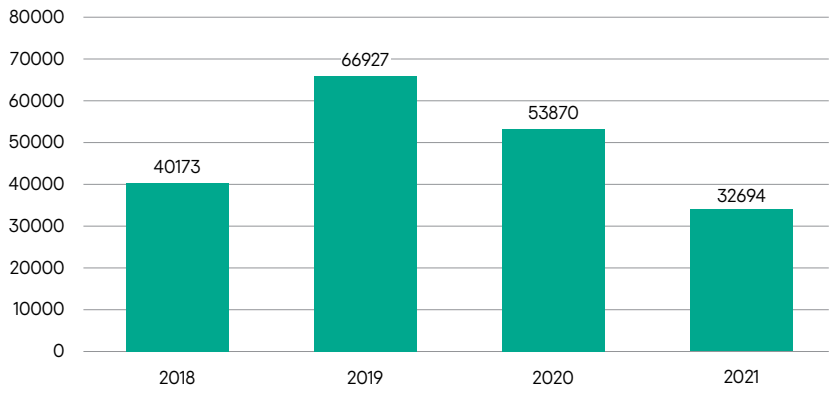
Tendencias observadas por Kaspersky

Cifras de detección global: usuarios afectados

En esta sección, detallamos las cifras regionales y globales observadas por Kaspersky en 2021 y las comparamos con las de años anteriores.

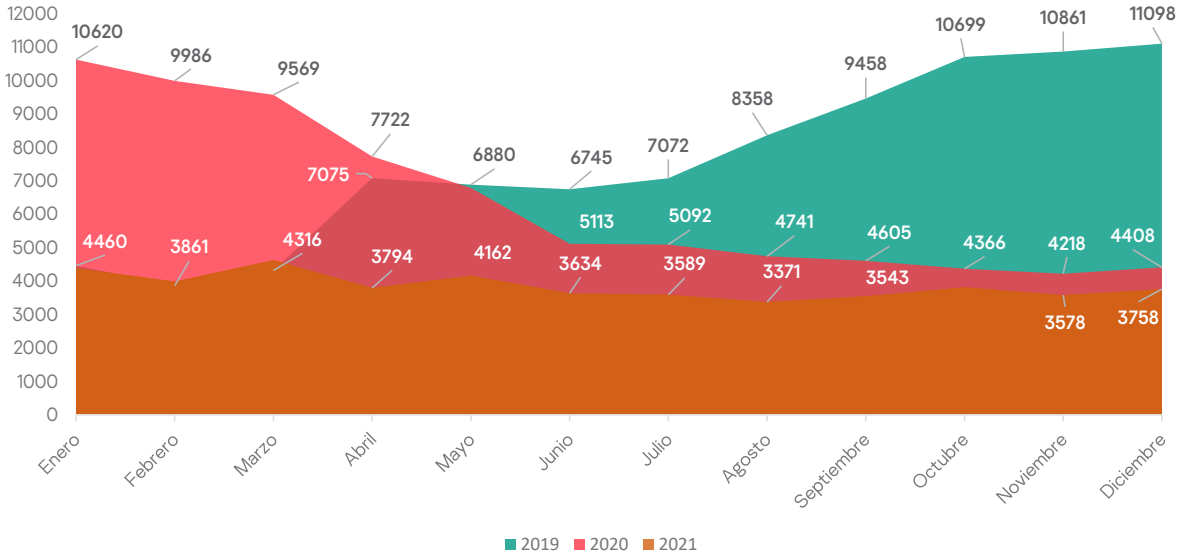
En 2021, un total de 32 694 usuarios fueron afectados por stalkerware

En 2021, un total de 32 694 usuarios fueron afectados por stalkerware. El siguiente gráfico muestra la evolución de los usuarios afectados año tras año desde 2018.



Evolución de los usuarios afectados año tras año desde 2018

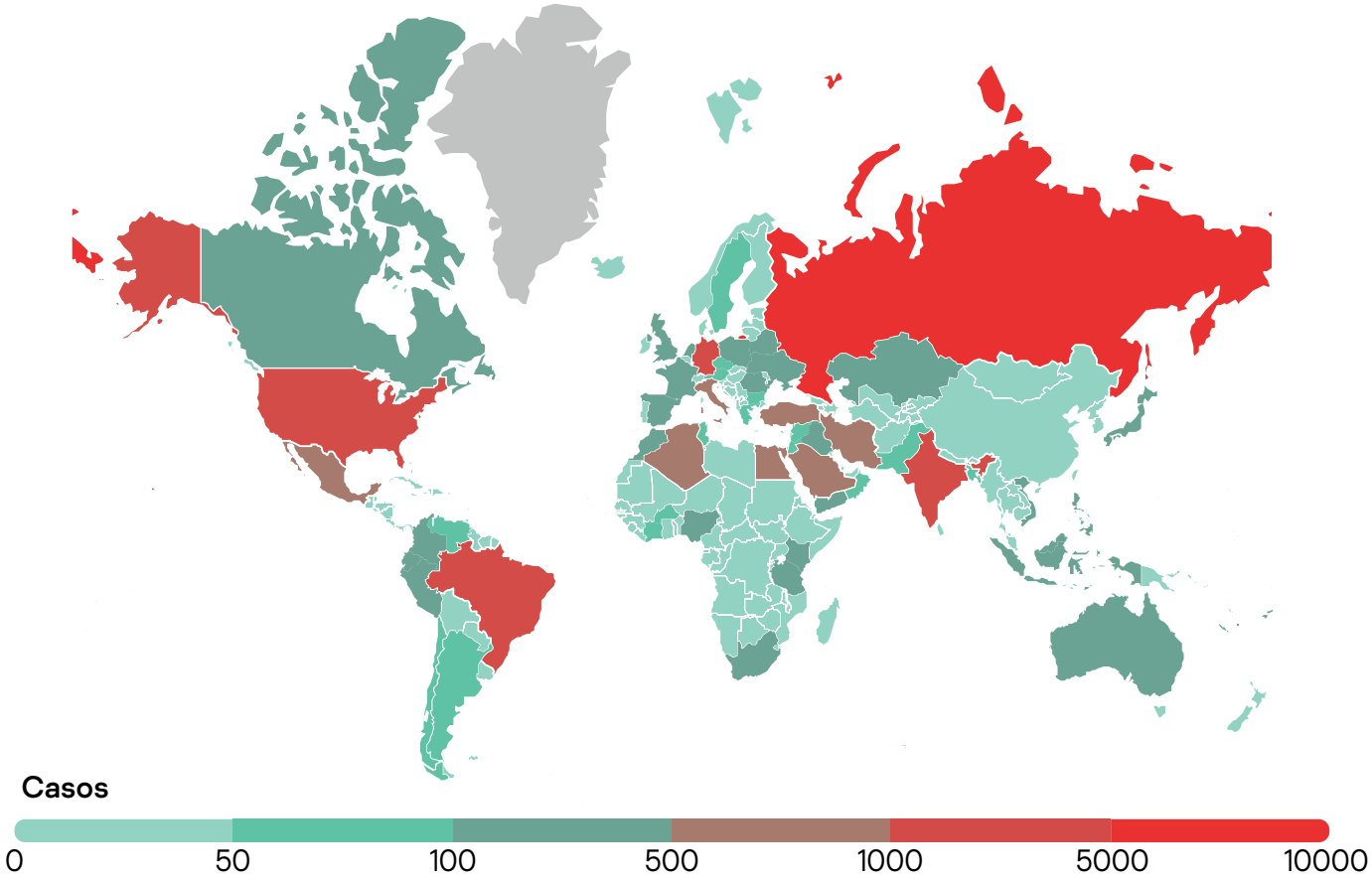
El siguiente gráfico muestra los usuarios únicos afectados por mes durante el periodo comprendido entre 2019 y 2021. Podemos observar que, en 2021, la tendencia fue más estable que en 2020, donde puede verse una disminución durante los meses más duros del confinamiento y las medidas de cuarentena.



Usuarios afectados únicos por mes durante el periodo comprendido entre 2019 y 2021

Cifras de detección global y regional: ubicación geográfica de los usuarios afectados

El stalkerware sigue afectando a personas de todo el mundo: en 2021, Kaspersky detectó usuarios afectados en 185 países o territorios.



Metodología

Los datos de este informe proceden de la suma de las estadísticas de amenazas obtenidas de Kaspersky Security Network. Kaspersky Security Network se dedica a procesar flujos de datos relacionados con ciberseguridad procedentes de millones de participantes voluntarios de todo el mundo. Todos los datos recibidos son anónimos. Para calcular nuestras estadísticas, revisamos la línea de consumo de las soluciones de seguridad para móviles de Kaspersky, aplicando solo los criterios de detección de stalkerware de la Coalition Against Stalkerware. Esto significa que el número de usuarios afectados solo fueron objetivo de stalkerware. Las estadísticas excluyen los tipos de aplicaciones de spyware o supervisión que no estén incluidas en la definición proporcionada por la coalición.

Estas reflejan el número de usuarios únicos de móviles afectados por stalkerware, lo que es diferente del número de detecciones. El número de detecciones podría ser mayor, ya que es posible que hayamos detectado stalkerware varias veces en el mismo dispositivo de un usuario único si este decidió no eliminar la aplicación tras recibir nuestra notificación.

Finalmente, las estadísticas reflejan únicamente a los usuarios móviles que utilizan las soluciones de seguridad de TI de Kaspersky. Es posible que algunos usuarios utilicen otras soluciones de ciberseguridad en sus dispositivos, mientras que otros no usen ninguna.

Al igual que en 2020, Rusia, Brasil, Estados Unidos e India vuelven a ser los cuatro países con el mayor número de usuarios únicos afectados. Resulta también interesante la caída de México del quinto al noveno puesto, y la entrada de Argelia, Turquía y Egipto entre los 10 más afectados. Han sustituido a Italia, Reino Unido y Arabia Saudí, que ya no forman parte de los 10 países más afectados por el stalkerware.

	País	Usuarios afectados
1	Rusia	7541
2	Brasil	4807
3	Estados Unidos	2319
4	India	2105
5	Alemania	1012
6	Irán (República Islámica de)	891
7	Argelia	665
8	Turquía	660
9	México	657
10	Egipto	640

Tabla 1: Los 10 países más afectados por stalkerware en 2021 en todo el mundo

En el informe de este año, ofrecemos estadísticas regionales más detalladas con cifras para Europa, Asia Pacífico, Latinoamérica, Norteamérica, Europa del Este (excluyendo los países de la UE), Rusia y Asia Central, y Oriente Medio y África.

En Europa, el número total de usuarios únicos afectados fue de 4236 en 2021. Alemania, Italia y Reino Unido ocupan los primeros puestos de la lista y vuelven a repetir sus puestos del año anterior. La República Checa ha sustituido a Austria entre los 10 primeros.

	País	Usuarios afectados
1	Alemania	1012
2	Italia	611
3	Reino Unido de Gran Bretaña e Irlanda del Norte	430
4	Francia	410
5	Polonia	321
6	España	321
7	Países Bajos	165
8	Rumanía	125
9	Bélgica	94
10	República Checa	82

Tabla 2: Los 10 países más afectados por el stalkerware en 2021 en Europa

En Europa del Este (excluyendo los países de la UE), Rusia y Asia Central, el número total de usuarios únicos afectados fue 9207. Los tres países más afectados fueron Rusia, Ucrania y Kazajistán.

	País	Usuarios afectados
1	Rusia	7541
2	Ucrania	490
3	Kazajistán	461
4	Bielorrusia	250
5	Uzbekistán	223
6	Azerbaiyán	92
7	República de Moldavia	51
8	Tayikistán	49
9	Kirguistán	40
10	Turkmenistán	19

Tabla 3: Los 10 países más afectados en 2021 por stalkerware en Europa del Este (excluyendo los países de la UE), Rusia y Asia Central

En la región de Oriente Medio y África, el número total de usuarios afectados en toda la región fue de 6270. Turquía, Egipto y Arabia Saudí fueron los países con el mayor número de afectados.

	País	Usuarios afectados
1	Turquía	660
2	Egipto	640
3	Arabia Saudí	575
4	Kenia	271
5	Sudáfrica	240
6	Emiratos Árabes Unidos	143
7	Nigeria	123
8	Kuwait	68
9	Omán	58
10	Etiopía	46

Tabla 4: Los 10 países más afectados por stalkerware en 2021, Medio oriente y África

En la región APAC, el número total de usuarios afectados fue de 4243. India fue con diferencia el país más afectado, con 2105 usuarios únicos. Le siguieron Indonesia y Vietnam.

	País	Usuarios afectados
1	India	2105
2	Indonesia	353
3	Vietnam	258
4	Filipinas	240
5	Malasia	229
6	Australia	205
7	Bangladés	169
8	Japón	167
9	Pakistán	98
10	Sri Lanka	83

Tabla 5: Los 10 países más afectados por stalkerware en 2021 en Asia Pacífico

La región de Latinoamérica y el Caribe estuvo dominada por un país: Brasil, que representó el 72,5% el número total de usuarios afectados en la región (y tan solo representa el 32 % de la población total de la región). A Brasil le siguieron México y Colombia. La región al completo tuvo un total de 6609 usuarios afectados.

	País	Usuarios afectados
1	Brasil	4807
2	México	657
3	Colombia	202
4	Ecuador	192
5	Perú	179
6	Argentina	90
7	Chile	73
8	Venezuela	58
9	Bolivia	46
10	Haití	36

Tabla 6: Los 10 países más afectados por stalkerware en 2021 en Latinoamérica

Por último, en Norteamérica, Estados Unidos representó el 87 % de usuarios afectados en la región, lo cual era de esperar ya que su población es 10 veces mayor que la de Canadá. El número total de afectados en Norteamérica, excluyendo a México, que se ha incluido en los datos de Latinoamérica, es de 2666.

	País	Usuarios afectados
1	Estados Unidos	2319
2	Canadá	347

Tabla 7: Usuarios de 2021 afectados por stalkerware – América del Norte

Funciones comunes de las aplicaciones de Stalkerware

Esta sección enumera las aplicaciones de stalkerware más utilizadas para controlar los dispositivos móviles a nivel global. Cerberus y Reptilicus fueron las aplicaciones de stalkerware más utilizadas, con 5575 y 4417 usuarios afectados, respectivamente, en todo el mundo.

	Nombre de la aplicación	Usuarios afectados
1	Cerberus	5,575
2	Reptilicus (o Vkurse)	4,417
3	Track My Phones	1,919
4	AndroidLost	1,731
5	MobileTracker Free	1670
6	Hoverwatch	1,094
7	wSpy	1,050

Tabla 8: Las principales aplicaciones de stalkerware en 2021

Las aplicaciones de stalkerware ofrecen gran capacidad de control y acceso a los usuarios, en función de la aplicación y de si se utiliza la versión gratuita o de pago. Algunas se comercializan como aplicaciones de control parental o antirrobo, pero son diferentes en muchos aspectos, empezando por el hecho de que funcionan en modo sigilo sin el consentimiento ni el conocimiento de la víctima.

Las aplicaciones mas populares ofrecen funciones de stalkerware tales como:

- Ocultar el icono de la aplicación
- Leer mensajes SMS, MMS y registros de llamadas
- Obtener listas de contactos

¿Afecta el stalkerware de la misma manera a sistemas operativos Android e iOS?

Las herramientas de stalkerware son menos frecuentes en iPhone que en teléfonos Android porque iOS es tradicionalmente un sistema cerrado. Aunque los agresores pueden evitar esta limitación en iPhones liberados, todavía requieren acceso físico directo al teléfono para liberarlo. Los usuarios de iPhone que quieran evitar que les vigilen no deberían perder nunca de vista su dispositivo.

De forma alternativa, un agresor puede ofrecer un iPhone (o cualquier otro dispositivo) a su víctima, con stalkerware ya instalado. Existen muchas empresas que ponen a disposición estos servicios online, lo que permite a los agresores instalar estas herramientas en nuevos teléfonos, que después ofrecen con el embalaje de fábrica a las víctimas como si fuera un regalo.

- Ubicación del GPS
- Eventos del calendario
- Leer mensajes de servicios y redes sociales, como Facebook, WhatsApp, Signal, Telegram, Viber, Instagram, Skype, Hangouts, Line, Kik, WeChat, Tinder, IMO, Gmail, Tango, SnapChat, Hike, TikTok, Kwai, Badoo, BBM, TextMe, Tumblr, Weico, Reddit etc.
- Visualizar fotos e imágenes de la galería del teléfono
- Realizar capturas de pantalla
- Captura de fotos con la cámara frontal (modo selfie)

Puede que el uso de stalkerware esté disminuyendo, pero la violencia no

El número de usuarios afectados y algunos de los comportamientos y percepciones sobre el uso de stalkerware siguen siendo preocupantes

Aunque hemos notado una disminución del 39 % en el número de usuarios afectados en comparación con los datos de 2020, la lucha contra el stalkerware y la ciberviolencia está lejos de haber llegado a su fin. El número de usuarios afectados y algunos de los comportamientos y percepciones sobre el uso de stalkerware siguen siendo preocupantes. En noviembre de 2021, Kaspersky realizó una encuesta global en la que participaron más de 21 000 personas de 21 países distintos para conocer su actitud hacia la privacidad y el acoso digital en relaciones íntimas. Aunque la mayoría de participantes (70 %) no cree que sea aceptable vigilar a su pareja sin su consentimiento, un porcentaje significativo (30 %) no lo ve como un problema y lo considera aceptable bajo ciertas circunstancias. Entre los que creían que existían razones justificables para la vigilancia secreta, casi dos tercios lo harían si creyesen que su pareja les estaba siendo infiel (64 %) o si estuviera relacionado con su seguridad (63 %), y la mitad de ellos si creyesen que su pareja participa en actividades delictivas (50 %).

Las tecnologías ICT son potentes herramientas para que los agresores puedan ejercer control coercitivo, especialmente en relaciones donde ya se daban casos de violencia física

La combinación de Internet de alta velocidad con la rápida difusión de la información y la tecnología de comunicación (ICT) ha respaldado la ciberviolencia al proporcionar una herramienta más con la que los agresores pueden compartir material peligroso o violento, así como poner en marcha comportamientos que causan daños emocionales, psicológicos o físicos. Aunque estas tecnologías permiten mantener relaciones emocionales y sociales a diferentes distancias físicas, ICT también ha permitido la ciberviolencia, una consecuencia cuyos efectos de gran envergadura se sienten también en el mundo offline, con un impacto negativo en las vidas de las víctimas.

Los resultados de nuestra encuesta corroboran esta información: un 15 % de los participantes de todo el mundo indica que su pareja le pidió instalar una aplicación de supervisión, y un 34 % de ellos también experimentó abusos verbales o físicos de su pareja.

Aunque es demasiado pronto para sacar conclusiones definitivas sobre el descenso de usuarios afectados en 2021, existen dos teorías que podrían explicar esta tendencia.

En primer lugar, creemos que todos los aspectos de nuestras vidas se siguen viendo muy afectados por la pandemia. Los estudios recientes muestran que están surgiendo nuevos comportamientos en diferentes áreas de nuestras vidas, como en el trabajo, en la enseñanza, en casa, en el consumo, en las comunicaciones y en la información, en los viajes y en la movilidad. En resumen, las personas pasan más tiempo en casa (el 49 % evita salir de casa y el 50 % teletrabaja a tiempo parcial o completo), reducen las interacciones cara a cara (el 57 % indica que mantiene la distancia social con amigos y la comunidad), y cada vez viajan, compran, estudian y se entretienen más online. Desde el punto de vista de un agresor, esto podría suponer una menor necesidad de espiar a su pareja, ya que puede verla la mayor parte del tiempo.

En segundo lugar, el Internet de las cosas (IoT) y la digitalización se han adentrado en todos los aspectos de nuestras vidas. Forma parte de nuestras rutinas diarias y oficinas, y de nuestros hogares y vehículos. Aunque las oportunidades y ventajas son infinitas, muchos dispositivos también permiten el seguimiento por parte de terceros. Nuestras investigaciones sugieren que los agresores también podrían utilizar otros medios aparte del stalkerware para vigilar a sus parejas, ya que el 50 % de los participantes en la encuesta indicó que les habían vigilado a través de aplicaciones para el teléfono, un 29 % a través de dispositivos de seguimiento, un 22 % mediante webcams y un 18 % a través de dispositivos inteligentes para el hogar.

La publicación de Apple en enero de 2022 de un manual de seguridad para sus productos AirTag indica un cambio en la percepción de la situación.

NNEDV, la red nacional para acabar con la violencia doméstica y WWP EN, la red europea para trabajar con agresores de violencia doméstica, compartieron con nosotros su experiencia y opiniones sobre estas dos teorías y sobre el abuso de la tecnología en general.

Cómo las medidas impuestas por los gobiernos durnate la pandemia ha facilitado y reforzado el control coercitivo — Berta Vall Castelló, directora de investigación y desarrollo y Anna McKenzie, directora de comunicación en WWP EN

El control coercitivo se define como "un patrón de comportamiento abusivo diseñado para ejercer control y dominio sobre la otra parte en una relación. Puede incluir diferentes comportamientos abusivos: físicos, psicológicos, emocionales o financieros, cuyo efecto acumulado impide que las víctimas-supervivientes ejerzan su autonomía e independencia como individuos" (McGorrery y McMahon, 2020). Como indicamos en nuestro manual "Misma violencia, nuevas herramientas: cómo trabajar con hombres que utilizan la ciberviolencia", los agresores aislan a sus parejas y hacen que se sientan emocionalmente dependientes. Emplean agresiones, amenazas, intimidación, humillación, aislamiento y otras tácticas para crear una constante sensación de miedo, así como un pérdida general de la sensación de libertad. Las tecnologías ICT son potentes herramientas para que los agresores puedan ejercer control coercitivo, especialmente en relaciones donde ya se daban casos de violencia física.

Un reciente informe sobre la violencia doméstica durante la pandemia de COVID-19 revela que las medidas impuestas por los gobiernos durante el confinamiento facilitaron y reforzaron el control coercitivo de los agresores. Se sugiere que las condiciones de aislamiento/distancia física impuestas por los gobiernos se solapan con las estrategias de control coercitivo que emplean los agresores para controlar a sus parejas (Pentaraki y Speake, 2020). Teniendo en cuenta estos resultados, parece posible que los agresores sientan menos "necesidad" de emplear stalkerware para ejercer control coercitivo sobre sus parejas. Además, las investigaciones recientes han observado que el abuso facilitado por la tecnología suele aumentar durante un periodo de separación (George y Harris 2014; Woodlock 2016). Por lo tanto, en una situación de confinamiento donde las parejas se ven forzadas a permanecer juntas en casa, son menos propensas a utilizar tecnología que permite el abuso.

WWP EN

La red europea para trabajar con agresores de violencia doméstica (WWP EN) es una asociación de miembros de organizaciones que trabaja de forma directa o indirecta con personas que ejercen violencia en relaciones estrechas. El principal objetivo de WWP EN es la violencia ejercida por hombres contra mujeres y niños. El objetivo de WWP EN es mejorar la seguridad de las mujeres y sus hijos, así como la de otras personas en riesgo de sufrir violencia en relaciones estrechas, mediante la promoción de trabajo efectivo con aquellos que ejercen esta violencia, en su mayoría hombres.

www.work-with-perpetrators.eu/experiencing-violence

Las medidas impuestas por los gobiernos durante el confinamiento facilitaron y reforzaron el control coercitivo de los agresores

Es importante recordar que la disminución del uso de stalkerware no equivale a un descenso de la violencia contra parejas íntimas durante la pandemia. Por el contrario, Boxal, Morgan y Brown (2020) indican que este tipo de violencia ha aumentado durante la pandemia de COVID-19. Por lo tanto, los resultados de este informe indican que el stalkerware ha sido reemplazado por otras herramientas. Tal y como indica Elena Gajotto, de la ONG italiana Una Casa per l'Uomo: "Supervisar y hacer seguimiento de una persona es muy fácil, por ejemplo con su cuenta de Google, por lo que no se necesita stalkerware". También es posible que la amplia variedad de tecnología que permite abusar de otra persona haya tenido un impacto en la disminución del stalkerware específicamente. Letizia Baroncelli, de la OGN italiana Centro Ascolto Uomini Malttratanti (CAM), se muestra de acuerdo y añade: "Creo que vamos a ver menos stalkerware porque existen muchas otras formas de ejercer abuso digital".

No obstante, tanto las ONG como los gobiernos y los investigadores han notificado un sustancial aumento del abuso y la extorsión sexual basada en imágenes desde el inicio de la pandemia (Boniello, 2020; CCRI, comunicación personal, 2 de junio de 2020; FBI, 2020, 2021). Parece que este tipo de abuso facilitado por la tecnología ha aumentado, sobre todo entre adolescentes y parejas que no viven juntas. Tal y como señala Letizia Baroncelli: "Compartir imágenes personales es una práctica que ha aumentado considerablemente desde la pandemia, sobre todo entre agresores jóvenes. No saben que están cometiendo un delito". Elena Gajotto añade: "El abuso basado en imágenes causa daños devastadores en las mujeres que lo sufren, mientras que los hombres ni siquiera se plantean que han hecho algo malo".

Varios miembros de WWP EN han compartido que la forma más común de violencia digital es la supervisión de las actividades digitales de la pareja, por ejemplo, leer correos electrónicos o revisar teléfonos y cuentas en redes sociales. Esto coincide con las observaciones de Daniel Antunovic, de la ONG croata UZOR, que indica también que las formas "primitivas" de acoso digital son las que ve que más frecuencia.

En WWP EN, consideramos que es fundamental centrarse en el abuso facilitado por la tecnología para garantizar la seguridad de la víctima. Elena Gajotto añade: "Cerca de la mitad de los hombres comparten su violencia digital, sin darse cuenta de que se trata de una forma de abuso. Si no nos centramos explícitamente en este tipo de violencia en el trabajo que hacemos con los agresores, no se darían cuenta". Por lo tanto, es necesario aumentar la capacidad de los profesionales que

trabajan con agresores y de los profesionales que trabajan con las víctimas de violencia doméstica para detectar e intervenir en casos de violencia digital. Daniel Antunovic señala además: "No hemos tratado con tantos casos de violencia digital como esperaba desde la COVID-19. No obstante, el abuso facilitado por la tecnología es, de alguna manera, como la violencia sexualizada. Sucede con frecuencia, pero permanece oculto".

NNEDV

El proyecto NNEDV Safety Net se centra en la intersección entre tecnología, privacidad, confidencialidad e innovación en lo que se refiere a la seguridad y el abuso mediante la promoción de políticas, la educación y la formación de defensores y profesionales en el sistema de justicia, y el trabajo con comunidades, agencias y empresas de tecnología para responder ante el abuso de la tecnología, apoyar a los supervivientes en el uso que hacen de la tecnología y aprovecharla para mejorar los servicios.

https://nnedv.org/content/mission-vision/

Cada vez son más los "dispositivos inteligentes" que se usan para ejercer violencia contra parejas íntimas — Toby Shulruff, gestor de proyectos de seguridad tecnológica en NNEDV

Aunque el stalkerware es una preocupación común, existen otras herramientas disponibles para ejercer violencia mediante la tecnología que pueden parecer stalkerware, aunque no lo sean. Por ejemplo, es posible usar la información personal disponible online y las funciones cotidianas de dispositivos y cuentas para encontrar la ubicación de una persona o hacer un seguimiento de su actividad. La complejidad y las conexiones entre dispositivos, cuentas e información disponible en Internet pueden impedir que las víctimas y las personas que trabajan con ellas identifiquen fácilmente qué está sucediendo para implementar una respuesta eficaz. Para un superviviente a este tipo de violencia puede resultar aterrador y abrumador darse cuenta de que el agresor conoce numerosos detalles de su día a día.

Lamentablemente, cada vez es mayor el número de dispositivos "inteligentes", como asistentes para el hogar, dispositivos conectados y sistemas de seguridad conectados a redes Wi-Fi y teléfonos móviles, que se usan en situaciones de violencia contra parejas íntimas.

En una encuesta realizada por NNEDV en diciembre de 2020 y enero de 2021, las respuestas mostraron un aumento en cada uno de los tipos de abuso tecnológico durante la pandemia. Si bien los teléfonos son la tecnología que más se usa de forma incorrecta (la evaluación de NNEDV demuestra que este es el caso el 87 % de las veces), también se identificaron los dispositivos conectados o "inteligentes" como tecnologías que cada vez más se usan incorrectamente, tal y como observan regularmente un tercio de los profesionales de apoyo.

Cada vez es mayor el número de dispositivos "inteligentes", como asistentes para el hogar, dispositivos conectados y sistemas de seguridad conectados a redes Wi-Fi y teléfonos móviles, que se usan en situaciones de violencia contra parejas íntimas

Como cada vez son más las personas que emplean este tipo de dispositivos IoT, lo más probable es que la tendencia vaya en aumento. El objetivo de estos productos es aumentar la comodidad y la eficacia. La fabricación de dispositivos IoT se ha convertido en un mercado rápidamente emergente tanto para empresas grandes y consolidadas como para empresas nuevas[1] y de menor tamaño. El IoT es posible gracias a la superposición de varias tendencias tecnológicas: la miniaturización, el aumento de la capacidad de procesamiento, el aumento del almacenamiento de datos, la reducción de los gastos de fabricación y la conectividad.

Debido a varios factores, como la presión en el mercado, la rápida emergencia de la tecnología y la complejidad del IoT, cada vez son más evidentes[2] los graves riesgos de seguridad y privacidad. En concreto, los dispositivos inteligentes para el hogar se utilizan de forma inadecuada en el contexto de la violencia contra parejas íntimas para controlar, amenazar y causar daño a las víctimas. [Los investigadores del proyecto Gender + IoT de University College London[3] han estado analizando estos daños] [y proponiendo soluciones en asociación con profesionales de apoyo en el campo.]

La reciente evaluación de necesidades de NNEDV documentó un aumento de la tecnología entre las tácticas de abuso durante la pandemia. Nos preocupa que a medida que superamos esta crisis de salud pública, los agresores que han adoptado estas tácticas o aumentado el uso indebido de la tecnología durante este tiempo, no encuentren un incentivo para dejar de llevar a cabo este tipo de abuso. Las investigaciones[4] recientes indican que los profesionales de apoyo deberían hacer preguntas sobre todos los tipos de abuso de la tecnología, incluido el stalkerware y los dispositivos domésticos inteligentes. Existe una gran probabilidad de que el aumento en el abuso tecnológico que han observado los profesionales de apoyo haya llegado para quedarse. Es esencial que sigamos apoyando a las víctimas y que nos esforcemos para prevenir el abuso de la tecnología.

1 Internet Society. (2015). The Internet of Things: An overview. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf or https://www.internetsociety.org/iot/

2 Internet Society. (2015). The Internet of Things: An overview. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf or https://www.internetsociety.org/iot/

3 Tanczer, L., Neira, I. L., Parkin, S., Patel, T., & Danezis, G. (2018). The rise of the Internet of Things and implications for technology-facilitated abuse. University College London.

4 Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. Proceedings of the ACM on human-computer interaction, 1 (CSCW), p.1-22.

Cómo colaboran Kaspersky y sus socios para luchar contra el stalkerware

La amenaza del stalkerware no solo es un problema técnico: todas las facetas de la sociedad deben involucrarse para resolver el problema. Durante los últimos años, Kaspersky ha liderado el debate sobre el stalkerware. Nos ponemos en contacto con partes interesadas públicas y privadas para comprender mejor el problema y buscar soluciones comunes. Contribuimos al desarrollo de materiales de formación y herramientas prácticas para apoyar a las organizaciones sin ánimo de lucro, las corporaciones, las instituciones y a las personas individuales a desarrollar resiliencia frente al stalkerware. Organizamos y participamos en seminarios web y mesas redondas con instituciones para compartir nuestra opinión y contribuir al debate que dará forma a la legislación del futuro.

Kaspersky es uno de los fundadores e impulsores de Coalition Against Stalkerware (CAS), un grupo de trabajo internacional dedicado a hacer frente al stalkerware y a combatir la violencia doméstica. La coalición reúne a organizaciones que trabajan con víctimas y agresores, activistas digitales y proveedores de ciberseguridad. Se trata de una plataforma única que permite a todas las partes interesadas compartir sus prácticas recomendadas y colaborar para hacer frente al problema del stalkerware.

Kaspersky también es uno de los socios del proyecto DeStalk. Financiado por la Comisión Europea, este proyecto de investigación tiene como objetivo desarrollar una estrategia para formar y apoyar a los profesionales que trabajan en servicios de apoyo a las víctimas y programas para agresores, empleados de instituciones y gobiernos locales, junto con otros grupos relevantes. El consorcio planea actualizar y probar las herramientas existentes para practicantes y está desarrollando una campaña piloto de concienciación regional en Italia.

En 2021, nos asociamos con INTERPOL y dos organizaciones sin ánimo de lucro de EE. UU. y Australia para proporcionar a los agentes de policía dos sesiones de formación online. A los cursos asistieron más de 210 participantes de todo el mundo.

A finales de 2021, Kaspersky también participó en el evento "Combating violence against women in a digital age - utilising the Istanbul Convention" (combatir la violencia contra las mujeres en la era digital: Convención de Estambul), organizada por el Consejo Europeo. Este evento fue una oportunidad para debatir las recomendaciones del grupo de expertos sobre cómo combatir la violencia contra la mujer y la violencia doméstica (GREVIO).

TinyCheck: una herramienta para apoyar a las víctimas de la violencia doméstica

TinyCheck es una herramienta gratuita y de código abierto desarrollada y apoyada por Kaspersky. Creada inicialmente para ayudar a las organizaciones sin ánimo de lucro a proteger a las víctimas de la violencia doméstica y su privacidad, TinyCheck permite detectar el stalkerware en los dispositivos de las víctimas y en cualquier sistema operativo de forma rápida, sencilla y no invasiva sin alertar al agresor. Si bien las soluciones de seguridad también pueden buscar stalkerware y alertar sobre su presencia, es necesario instalarlas en el dispositivo, por lo que existe el riesgo de que el agresor también sea alertado.

TinyCheck permite detectar el stalkerware en los dispositivos y en cualquier sistema operativo de forma rápida, sencilla y no invasiva, sin alertar al agresor

TinyCheck no requiere la instalación de ninguna aplicación en el dispositivo para realizar el análisis, y los resultados no se muestran ni se transmiten a ningún dispositivo potencialmente infectado. Además, TinyCheck permite a las víctimas analizar cualquier dispositivo, independientemente de si usan iOS, Android o cualquier otro sistema operativo. Estas funciones abordan los dos principales problemas a la hora de proteger a los usuarios del stalkerware. La herramienta se ha desarrollado para ejecutarse en una Raspberry Pi mediante una conexión Wi-Fi. TinyCheck analiza rápidamente el tráfico saliente de un dispositivo móvil e identifica los indicadores de compromiso, como interacciones con fuentes maliciosas conocidas, como los servidores relacionados con stalkerware. Actualmente, la herramienta utiliza indicadores de compromiso recopilados tanto por los investigadores de Kaspersky como por repositorios mantenidos por investigadores de seguridad independientes (con agradecimiento especial a Etienne Maynier, también conocido como Tek, de Echap y a Cian Heasley). Esperamos que la comunidad continúe este trabajo manteniendo estos indicadores actualizados.

Dicho esto, también es importante conocer las limitaciones de TinyCheck. La herramienta debe usarse teniendo en cuenta la siguiente advertencia: los indicadores de compromiso no proporcionan detección completa en tiempo real de todas las aplicaciones de stalkerware como haría una solución de seguridad de TI. Por lo tanto, un resultado que no haya detectado stalkerware no excluye la posibilidad de que se ha instalado este tipo de software pero que TinyCheck no lo haya reconocido.

En 2021, más organizaciones sin ánimo de lucro del ámbito de la violencia doméstica probaron TinyCheck y proporcionaron comentarios para mejorar el servicio. Las fuerzas policiales y los organismos judiciales de varios países también se han interesado en la herramienta para apoyar mejor a las víctimas.

En 2021 fuimos testigos de avances positivos en los frentes institucionales y reguladores

Durante 2021 se han observado en todo el mundo avances positivos en la lucha contra el stalkerware desde el punto de vista institucional y normativo. En mayo de 2021, el parlamento japonés promulgó una propuesta de ley para enmendar la ley sobre regulación del acoso. De acuerdo con esta enmienda, además de otras estipulaciones, obtener la información de ubicación de los teléfonos inteligentes de la gente sin autorización se considera ilegal.

En agosto de 2021, la Comisión Federal del Comercio de Estados Unidos prohibió a un fabricante de aplicaciones ofrecer stalkerware. Fue la primera prohibición de este tipo.

El 17 de agosto de 2021, el Bundestag alemán aprobó la "Ley para enmendar el código criminal: combatir de forma más eficaz el acoso y mejorar la cobertura del ciberacoso" (traducido del alemán). La nueva ley entró en vigor el 1 de octubre de 2021 y ahora incluye el ciberacoso en su catálogo de ofensas. El cambio se debe al continuo progreso tecnológico y al riesgo asociado de sufrir ciberacoso, en concreto a través de aplicaciones diseñadas para este fin o stalkerware. Además, un aspecto importante de la nueva ley es que clasifica un caso como serio si el agresor "en el curso de una ofensa, emplea un programa informático cuyo propósito es espiar de forma digital a otras personas".

El Consejo de Europa ha estado muy activo sobre este tema en 2021. En su primera recomendación sobre la "dimensión digital" de la violencia contra la mujer, el grupo de expertos del Consejo de Europa para la acción frente a la violencia contra la mujer y la violencia doméstica (GREVIO por sus siglas en inglés) define y señala tanto los problemas de la violencia de género contra la mujer que se comete online como los ataques contra la mujer mediante el uso de la tecnología, como dispositivos de seguimiento de obtención legal que permiten a los agresores acechar a sus víctimas. A esta recomendación le siguió en diciembre de 2021 un informe de iniciativa legislativa sobre la ciberviolencia basada en género que fue adoptado por el Parlamento Europeo. El informe apela a la (i) creación de una definición común de ciberviolencia basada en género y al (ii) desarrollo de capacidades para las partes interesadas. Destaca el stalkerware entre otros medios clave para la ciberviolencia y "rechaza la noción de que las aplicaciones de stalkerware se puedan considerar aplicaciones de control parental". Tras las recomendaciones generales del Consejo de Europa, este

informe, aunque no es vinculante, es otro documento oficial positivo donde se menciona el problema del stalkerware e impulsa a los estados miembros a adaptar sus legislaciones y acciones para abordar el problema. Finalmente, el 8 de marzo de 2022, la Comisión Europea publicó una propuesta para una directiva del Parlamento Europeo y el Consejo para combatir la violencia contra la mujer y la violencia doméstica. El documento trata la ciberviolencia y dedica dos artículos al ciberacoso (Art 8) y al ciberhostigamiento (Art 9) que propone criminalizar.

¿Cree que es una víctima de stalkerware? Aquí encontrará unos cuantos consejos

Si necesitas ayuda, acude a una organización de apoyo local. Para encontrar una cerca de ti, consulta el sitio web de la Coalición contra el Stalkerware

Tanto si es una víctima de stalkerware como si no, a continuación encontrará varios consejos para protegerse mejor:

- Proteja su teléfono con una contraseña segura y nunca la comparta con su pareja, amigos ni compañeros de trabajo
- Cambie las contraseñas de todas sus cuentas de forma periódica y no las comparta con nadie
- Descargue aplicaciones únicamente de fuentes oficiales, como Google Play o Apple App Store
- Instale una solución de seguridad de TI fiable como Kaspersky Internet Security for Android en sus dispositivos y analícelos de forma periódica. Sin embargo, si ya se ha podido instalar stalkerware, solo debería usar una solución de este tipo tras evaluar el riesgo para la víctima, ya que el agresor podría darse cuenta del uso de una solución de ciberseguridad.

Las víctimas de stalkerware podrían ser víctimas de un ciclo de abuso más amplio, que podría ser también físico. En algunos casos, el agresor recibe una notificación si la víctima analiza el dispositivo o elimina una aplicación de stalkerware. Si esto sucede, puede empeorar la situación y aumentar la agresión. Por eso, es importante actuar con precaución si piensa que es objetivo de stalkerware.

- **Póngase en contacto con una organización de apoyo local:** para encontrar la más cercana, eche un vistazo al sitio web de Coalition Against Stalkerware.
- **No pierda de vista los siguientes signos de advertencia:** la batería se agota rápidamente por aplicaciones desconocidas o sospechosas, o aparición de aplicaciones recientemente instaladas con acceso sospechoso al uso y seguimiento de su ubicación, al envío o recepción de mensajes y a otras actividades personales. Compruebe también si el ajuste "fuentes desconocidas" está activado, ya que podría indicar que se ha instalado software no deseado de una fuente externa. Es importante recordar que las señales indicadas anteriormente son solo síntomas de la posible instalación de stalkerware y no una indicación definitiva.
- **No intente borrar el stalkerware, cambiar los ajustes ni manipular el teléfono:** estas acciones podrían alertar al posible agresor y empeorar la situación. Además, corre el riesgo de eliminar datos o pruebas importantes que podrían utilizarse en un juicio.

Para más información sobre nuestras actividades en materia de stalkerware o cualquier otra solicitud, escríbanos a ExtR@kaspersky.com.

La Coalición contra el Stalkerware se fundó en noviembre de 2019 como respuesta a la creciente amenaza creada por el stalkerware. La Coalición busca combinar la experiencia de sus socios en el ámbito de la asistencia a los supervivientes de violencia doméstica con el trabajo con la persona que ha perpetrado el abuso y la defensa de los derechos digitales. Todos los miembros tienen el firme compromiso de luchar contra la violencia doméstica, el acoso y el acecho abordando la utilización de stalkerware y creando conciencia pública sobre este problema.

Coalición contra el Stalkerware:
https://stopstalkerware.org/

COALITION AGAINST STALKERWARE

Noticias sobre ciberamenazas: www.securelist.lat
Noticias de seguridad: business.kaspersky.com
Seguridad para PYMEs:
www.kaspersky.es/small-to-medium-business-security
Seguridad para grandes empresas:
www.kaspersky.es/enterprise-security

www.kaspersky.es

kaspersky