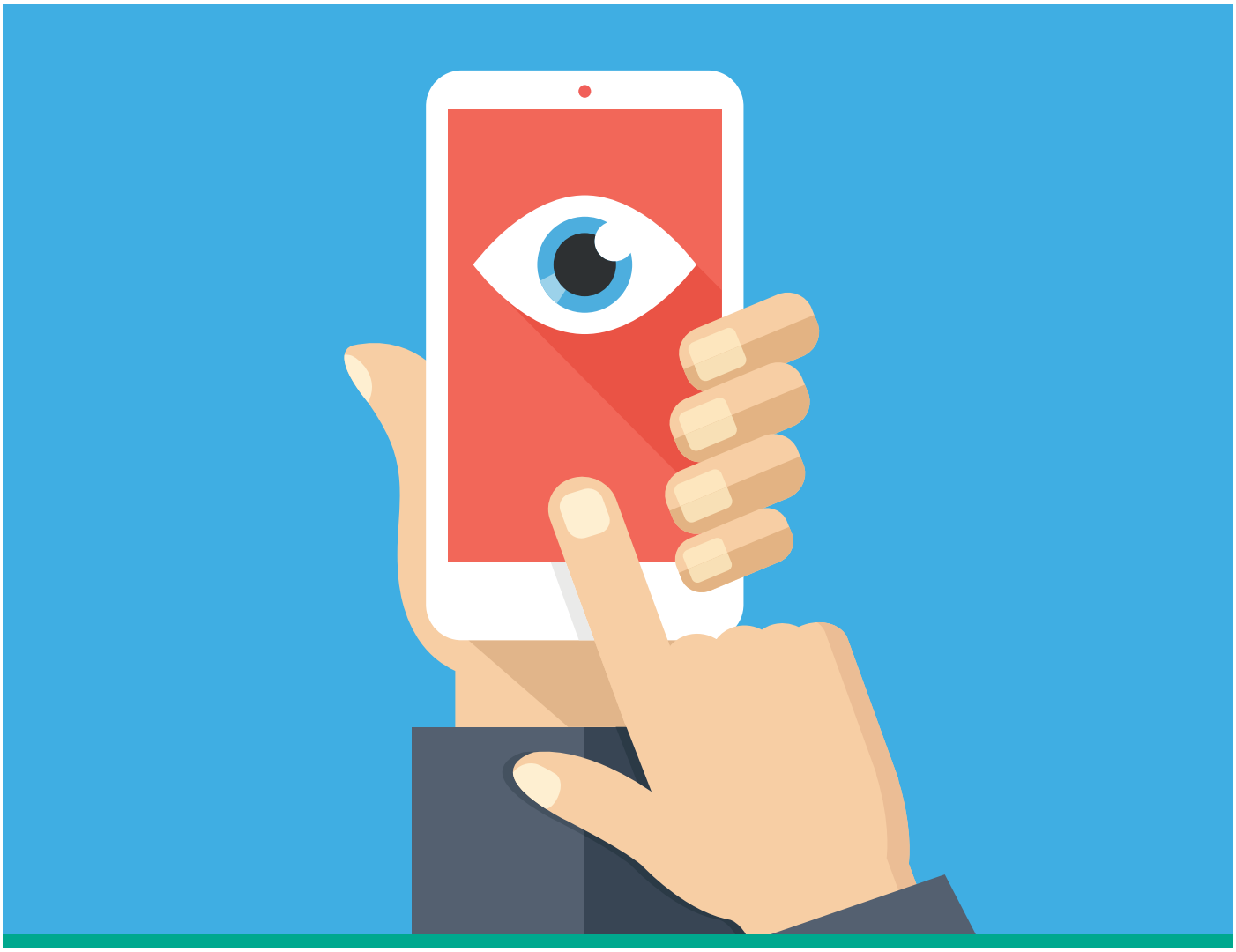


La situación del **stalkerware** en 2020

COALITION AGAINST STALKERWARE

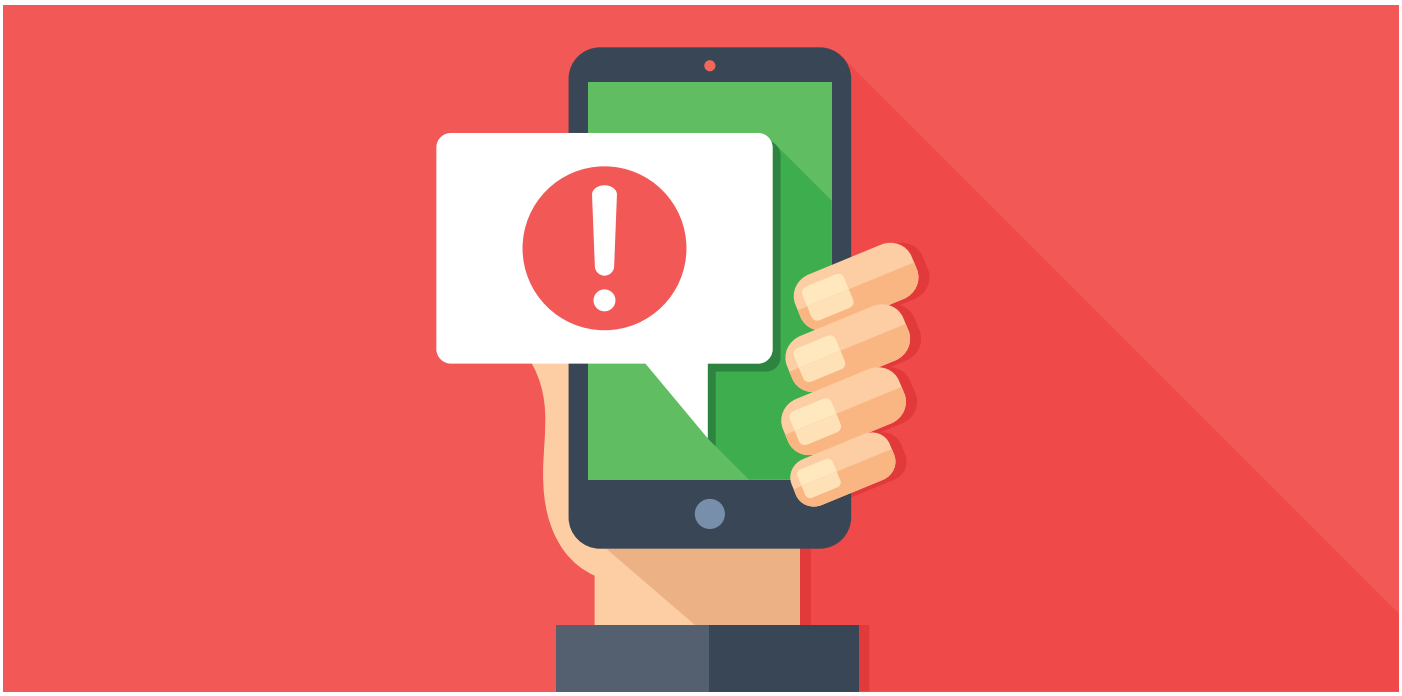
kaspersky

Índice

Principales conclusiones de 2020

Los datos de Kaspersky muestran que la escala del problema del stalkerware no ha mejorado mucho en 2020 en comparación con el último año:

- El número de personas afectadas sigue siendo elevado. En total, 53 870 de nuestros usuarios móviles se vieron afectados por stalkerware en 2020 en todo el mundo. Teniendo en cuenta la situación general, estas cifras solo se corresponden con los usuarios de Kaspersky, por lo que las cifras totales a escala mundial serían aún superiores. Algunos usuarios afectados pueden usar otra solución de seguridad informática en sus dispositivos, y puede que haya otros que no usen ninguna.
- Con más de 8100 usuarios afectados en todo el mundo, Nidb es la muestra de stalkerware más usada, según nuestras estadísticas de 2020. Esta muestra se utiliza para vender diversos productos de stalkerware, como iSpyoo, TheTruthSpy y Copy9, entre otros.
- En lo que respecta a la expansión geográfica, observamos la aparición de una tendencia bastante sólida: Rusia, Brasil y Estados Unidos siguen siendo los países más afectados de todo el mundo, y son los tres países que lideran la clasificación en 2020.
- En Europa, Alemania, Italia y el Reino Unido son los tres países más afectados respectivamente.



Introducción y metodología

La tecnología ha permitido que las personas se conecten más que nunca. Podemos compartir de manera digital nuestras vidas con nuestra pareja, nuestra familia y nuestros amigos independientemente de la distancia física. También estamos observando un aumento de la aparición de software que permite a los usuarios espiar de forma remota la vida de otra persona desde su dispositivo digital sin que el usuario afectado haya dado su consentimiento e incluso sin que este lo sepa.

Los riesgos que conlleva el stalkerware pueden traspasar la esfera de Internet y alcanzar el mundo físico. La Coalición contra Stalkerware advierte de que el stalkerware «puede facilitar el control, acoso, abuso y violencia en la pareja».

Este software, conocido como stalkerware, puede ser adquirido por cualquier persona con acceso a Internet. Los riesgos que conlleva el stalkerware pueden traspasar la esfera de Internet y alcanzar el mundo físico. La Coalición contra Stalkerware advierte de que el stalkerware «puede facilitar el control, acoso, abuso y violencia en la pareja». Además, el stalkerware puede funcionar en modo invisible, es decir, no aparece ningún icono en el dispositivo que indique su presencia y no es visible para el usuario afectado. La mayoría de usuarios afectados ni siquiera sabe que existe este tipo de software. Eso quiere decir que no pueden protegerse, ni en línea ni cuando están sin conexión, sobre todo porque el responsable que usa stalkerware suele conocer a la víctima personalmente.

En los últimos años, Kaspersky ha estado trabajando de forma activa con algunos socios para terminar con el uso de stalkerware. En 2019, creamos una alerta especial que avisa a los usuarios si se instala algún tipo de stalkerware en sus móviles. Después de eso, nos convertimos en uno de los diez miembros fundadores de la Coalición contra Stalkerware. También publicamos nuestro primer informe completo sobre la situación del stalkerware en el mismo año para comprender la dimensión del problema.

En este informe, seguimos analizando el asunto del stalkerware y presentamos nuevas estadísticas de 2020, con el fin de compararlas con los datos anteriores. Los datos de este informe se han obtenido a partir de estadísticas agregadas de amenazas de Kaspersky Security Network. Kaspersky Security Network se basa en procesar flujos de datos relacionados con la seguridad informática de millones de participantes voluntarios de todo el mundo. Todos los datos recibidos se anonimizan. Para calcular nuestras estadísticas, revisamos la línea de asistencia al consumidor de las soluciones de seguridad móviles de Kasperksy.

El problema del stalkerware y la historia subyacente

El stalkerware es un software que cualquier persona con acceso a Internet puede comprar. Se usa para espiar de forma remota a otra persona desde su dispositivo sin que el usuario afectado haya dado su consentimiento e incluso sin que este lo sepa. El stalkerware puede funcionar en modo invisible, es decir, no aparece ningún icono en el dispositivo que indique su presencia y no es visible para el usuario afectado. Por ello, la Coalición contra Stalkerware define el stalkerware como un software que «puede facilitar el control, acoso, abuso y violencia en la pareja».

La dimensión de la ciberviolencia

En Europa, siete de cada diez mujeres que han sufrido ciberacoso, también han sufrido al menos una forma de violencia física o sexual por parte de su pareja.

Según un informe del Instituto Europeo de la Igualdad de Género, «en Europa, siete de cada diez mujeres que han sufrido ciberacoso, también han sufrido al menos una forma de violencia física o sexual por parte de su pareja». Haciéndose eco de estos datos, expertos de organizaciones sin ánimo de lucro que asisten a víctimas de violencia doméstica hacen hincapié en que ciberviolencia también es una forma de violencia. Al igual que ocurre con la violencia física, psicológica y económica, el agresor puede usar la vigilancia para obtener un control completo de su víctima/superviviente[1] y quedar al mando de la situación.

Mediante el stalkerware, el alcance del control que ejerce el agresor puede llegar a ser inmenso. En función del tipo de stalkerware instalado, este puede incluir una amplia variedad de funciones para inmiscuirse en la privacidad de la víctima. Con la ayuda de este software, el agresor puede:

- Leer todo lo que la persona vigilada escribe: se registran las pulsaciones de teclas del dispositivo, incluidas las credenciales de cualquier tipo de servicio, como aplicaciones de banca, tiendas en línea, redes sociales, etc.
- Saber dónde está: el agresor puede seguir los movimientos de una persona con GPS en tiempo real.
- Escuchar lo que dice: puede escuchar las llamadas o incluso grabarlas.
- Leer mensajes de cualquier servicio de mensajería, aunque este utilice tecnología de cifrado.

1 Los expertos usan cada vez más en su terminología «superviviente» en lugar de «víctima» con el fin de empoderar a las mujeres que sufren violencia. Por ese motivo, utilizamos ambos términos en este informe.

- Controlar la actividad en redes sociales.
- Ver fotos y vídeos.
- Encender la cámara.

Toda esta información privada se puede recopilar, normalmente desde un dispositivo móvil, como una tablet o un smartphone.

Las organizaciones sin ánimo de lucro de la Coalición contra Stalkerware se están encontrando con un número cada vez más alto de supervivientes que buscan ayuda para este problema.

Las organizaciones sin ánimo de lucro de la Coalición contra Stalkerware se están encontrando con un número cada vez más alto de supervivientes que buscan ayuda para este problema:

- Los resultados del Segundo Estudio Nacional sobre acoso a través de la tecnología y violencia doméstica en **Australia**, llevado a cabo por la Red de Servicios para la Mujer en Australia (WESNET) con la ayuda de la Dra. Delanie Woodlock e investigadores de la Universidad Curtin, confirman que el 99,3 % de los profesionales que tratan a víctimas de violencia doméstica asisten a personas que sufren acoso facilitado por la tecnología y que el uso de cámaras de vídeo aumentó en un 183,2 % entre 2015 y 2020.
- Según un estudio sobre violencia en Internet en relaciones de pareja, que llevó a cabo el Centre Hubertine Auclert en **Francia**, el 21 % de las víctimas ha vivido que sus parejas utilicen stalkerware, y el 69 % de las víctimas tiene la sensación de que su pareja ha accedido a la información personal de su smartphone a escondidas.
- En **Alemania**, durante muchos años, los centros de asesoramiento para mujeres y los centros de ayuda para víctimas de violación (bff) han experimentado un incremento en el uso de stalkerware en las relaciones de pareja.
- En los **EE. UU.**, el stalking afecta a un número estimado de entre 6-7,5 millones de personas en un periodo de un año, y una de cada cuatro víctimas afirma que ha sido acosada mediante algún tipo de tecnología, de acuerdo con el Stalking Prevention Awareness & Resource Center (SPARC).

El acceso físico es la clave

Lamentablemente, no es muy difícil instalar stalkerware de forma secreta en el teléfono de una víctima. El principal obstáculo es que el stalkerware tiene que configurarse en el dispositivo afectado. Debido al vector de distribución de este tipo de aplicaciones, que es muy distinto de los esquemas de distribución del malware común, es imposible que un dispositivo se infecte con stalkerware mediante un mensaje de spam, como un enlace a stalkerware o una trampa que la víctima encuentra mientras navega por Internet.

Esto quiere decir que el agresor necesita acceso físico al dispositivo para poder instalar el stalkerware. Esto es posible si el dispositivo no tiene PIN, patrón ni contraseña que lo proteja o si el agresor conoce a la víctima/superviviente personalmente. La instalación en el dispositivo se puede completar en unos minutos.

Antes de acceder al dispositivo de la superviviente, el agresor tiene que obtener un enlace al paquete de instalación desde la página web del desarrollador del stalkerware. En la mayoría de casos, el software no se descarga desde una tienda oficial de aplicaciones. En dispositivos Android, Google prohibió las aplicaciones que son claramente stalkerware en su tienda de aplicaciones Google Play en 2020. Esto quiere decir que el agresor no podrá instalar este tipo de aplicación desde una tienda de aplicaciones común. En su lugar, tendrá que seguir varios pasos antes de instalar el stalkerware. Por ello, es posible que el agresor deje algún rastro en los ajustes del dispositivo, y la víctima puede realizar algunas comprobaciones si le preocupa que puedan estar espiándola.

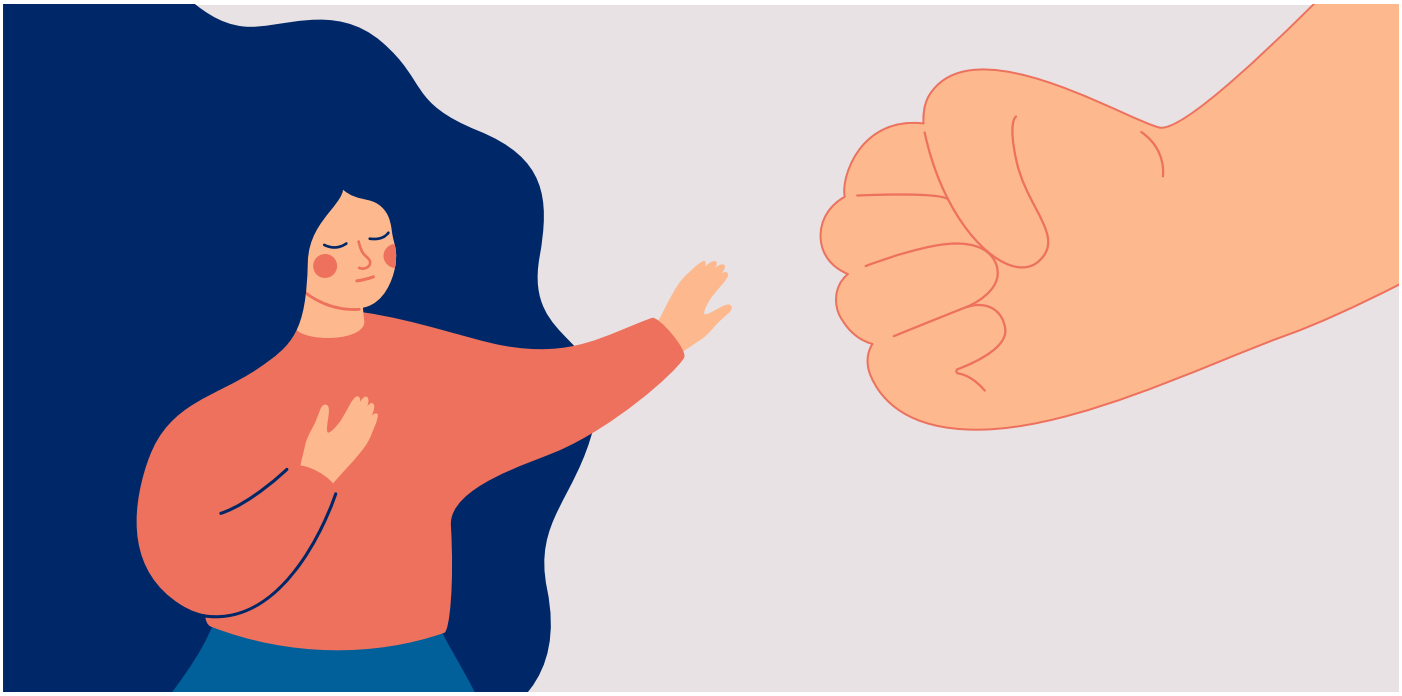
Las herramientas de stalkerware son menos frecuentes en dispositivos iPhone que en dispositivos Android.

Las herramientas de stalkerware son menos frecuentes en dispositivos iPhone que en dispositivos Android porque iOS suele ser un sistema cerrado. Sin embargo, los agresores pueden saltarse esta limitación en dispositivos iPhone con jailbreak. Se sigue necesitando acceso físico al teléfono para poder liberarlo mediante jailbreak, así que los usuarios de iPhone que temen que les espíen deben vigilar de cerca su dispositivo. También es posible que un agresor le regale a su víctima un iPhone (o algún otro dispositivo) con stalkerware preinstalado. Hay muchas empresas que ofrecen sus servicios en Internet para instalar este tipo de herramientas en un teléfono nuevo y enviárselo a alguien en su embalaje original para celebrar una ocasión especial.

El riesgo de perder la privacidad

La información que se controla desde el stalkerware estará disponible para al menos una persona: el agresor que ha instalado el software en el teléfono de la superviviente. Sin embargo, en ocasiones ocurre que todos los datos privados se hacen públicos. Año tras año, los servidores de stalkerware se ven comprometidos por la actuación de hackers o se dejan abiertos sin protección, lo que provoca que se pueda acceder a la información o que esta quede expuesta en Internet. Por ejemplo, en 2020, se produjo una vulneración de datos debido a un producto que facilitó ClevGuard. En años anteriores, ocurrieron incidentes similares con Mobiispy en 2019 y MSpy en 2018 y 2015.

Estos son solo algunos ejemplos de una larga lista de casos en los que las bases de datos de empresas que desarrollan stalkerware se han visto expuestas, afectando a millones de cuentas de usuario. La posibilidad de rastrear la ubicación de una persona no solo implica que esta pierda su privacidad en línea, sino que su seguridad en el plano físico también podría estar en riesgo.



Situación jurídica

Las empresas venden y ofrecen las aplicaciones de stalkerware bajo distintos pretextos: para supervisar a niños y niñas o como soluciones de seguimiento de empleados. Las leyes varían de un país o estado a otro, pero están empezando a llegar a un punto en común. Por norma general, solo es ilegal usar este tipo de herramientas y aplicaciones que registran la actividad de los usuarios si no se tiene su consentimiento o el de la autoridad jurídica. Poco a poco, estamos observando algunos cambios en la legislación. Por ejemplo, en 2020, Francia endureció las sanciones por vigilancia secreta: geolocalizar a alguien sin su consentimiento es ahora condenable con un año de prisión y una multa de 45 000 €. Si esta situación ocurre dentro de la pareja, las sanciones son mucho mayores, como dos años de prisión y una multa de 60 000 €.

Las herramientas de stalkerware infringen la ley con frecuencia y exponen al acosador a tener responsabilidad jurídica por grabaciones que haya realizado sin el consentimiento de la víctima. Los acosadores deben saber que están infringiendo la ley. Si se descubre el uso de stalkerware, la sanción se aplica al usuario privado que ha instalado el software, no al proveedor. En EE. UU., solo se ha sancionado a dos desarrolladores de aplicaciones para espiar en los últimos tiempos. Uno de ellos tuvo que pagar una multa de 500 000 dólares estadounidenses, lo que acabó con el proceso de desarrollo de la aplicación, y el otro recibió una orden que le obligaba a cambiar las funciones de la aplicación para seguir vendiéndola.

El alcance del problema

Cifras de detección a nivel mundial: usuarios afectados

En total, 53 870 usuarios se vieron afectados por stalkerware en 2020 en todo el mundo. Mientras que 67 500 usuarios se vieron afectados en 2019 en todo el mundo.

En esta sección, analizamos cifras globales de usuarios únicos que han descubierto que su dispositivo móvil tenía instalado stalkerware.

Los datos de 2020 demuestran que la situación provocada por el uso de stalkerware no ha mejorado mucho: el número de personas afectadas sigue siendo alto. En total, 53 870 usuarios se vieron afectados por stalkerware en 2020 en todo el mundo. Mientras que 67 500 usuarios se vieron afectados en 2019 en todo el mundo. Sin embargo, hay que tener en cuenta que 2020 ha sido un año sin precedentes en el que nuestras vidas han cambiado drásticamente en todo el planeta.

Para combatir la pandemia de COVID-19, todos los países del mundo se han enfrentado a grandes restricciones, como medidas de autoaislamiento o confinamiento, para obligar a la gente a quedarse en casa. Teniendo en cuenta que el stalkerware es una herramienta más de control sobre la pareja con la que convive el agresor, esto podría explicar la disminución de las cifras en comparación con el año anterior.

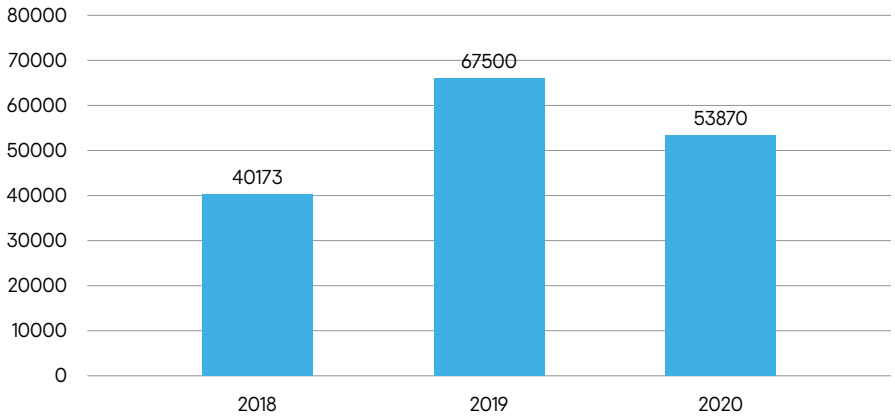


Tabla 1 Usuarios afectados por stalkerware en todo el mundo desde 2018 hasta 2020 (total anual)

Estos datos demuestran que las cifras de 2020 continúan en un nivel alto y estable. En comparación con 2018, se detectaron 40 173 casos de usuarios afectados en todo el mundo por stalkerware.

Cuando observamos las cifras del número total de usuarios únicos afectados por stalkerware en todo el mundo en 2020 mes a mes, esta tendencia se hace todavía más evidente. Los dos primeros meses del año fueron estables, con muchos casos de dispositivos afectados, demostrando así que el stalkerware era una herramienta bastante popular. La situación cambió en marzo, cuando muchos países decidieron anunciar medidas de cuarentena. La curva muestra una tendencia clara: los números empiezan a estabilizarse en junio de 2020, cuando en muchos países de todo el mundo se relajaron las restricciones.

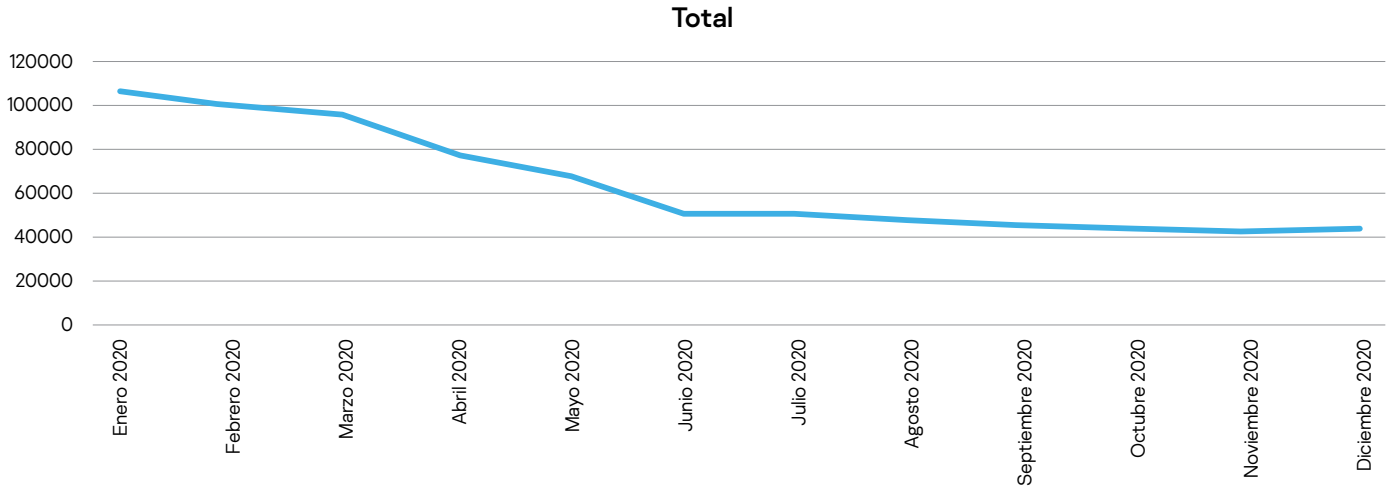


Tabla 2 Usuarios afectados por stalkerware en todo el mundo en 2020 (total al mes)

Estos datos demuestran que las cifras de 2020 continúan en un nivel alto y estable. En comparación con 2018, se detectaron 40 173 casos de usuarios afectados en todo el mundo por stalkerware. Esto pone en perspectiva las cifras totales de 2020, ya que hemos observado una integración más elevada de la tecnología en nuestras vidas. Por desgracia, esto también significa que cada vez es más común usar software para espiar como otro tipo más de violencia en la pareja.

Cifras de detección a nivel mundial: muestras de stalkerware

En esta sección, analizamos qué muestras de stalkerware son las más usadas para controlar dispositivos móviles a nivel mundial. En los siguientes resultados se pueden observar las muestras más detectadas en 2020:

	Muestras	Usuarios afectados
1	Monitor.AndroidOS.Nicb.a	8147
2	Monitor.AndroidOS.Cerberus.s	5429
3	Monitor.AndroidOS.Agent.af	2727
4	Monitor.AndroidOS.Anlost.a	2234
5	Monitor.AndroidOS.MobileTracker.c	2161
6	Monitor.AndroidOS.PhoneSpy.b	1774
7	Monitor.AndroidOS.Agent.hb	1463
8	Monitor.AndroidOS.Cerberus.a	1310
9	Monitor.AndroidOS.Reptilic.a	1302
10	Monitor.AndroidOS.SecretCam.a	1124

Tabla 3: Las 10 muestras de stalkerware más detectadas a nivel mundial en 2020

1. Con más de 8100 usuarios afectados, **Nidb** fue la muestra de stalkerware más usada en 2020. El creador de Nidb vende su producto de stalkerware como servicio. Esto significa que cualquier persona puede alquilar su software de servidor de control y su aplicación móvil, cambiarle el nombre para adecuarlo al mercado y venderlo de forma independiente. Algunos ejemplos de ello son iSpyoo, TheTruthSpy, Copy9 y otros.
2. El segundo y el octavo puesto están ocupados por Cerberus. Son dos muestras distintas dentro de la misma familia. La variante **Cerberus.a** ha afectado a más de 5400 usuarios.
3. Con más de 2700 usuarios afectados, **Agent.af** se coloca en tercer lugar. Se vende como Track My Phone, y tiene funciones típicas como la lectura de mensajes de cualquier servicio de mensajería, el registro del historial de llamadas de una persona y el seguimiento de la localización.
4. **Anlost.a** es un buen ejemplo de stalkerware de incógnito. Se vende como una aplicación antirrobo, y su icono se ve en la pantalla de inicio (algo que no es común en aplicaciones de stalkerware sigilosas). Por tanto, está disponible en Google Play Store. Es decir, es posible ocultar deliberadamente el icono en la pantalla de inicio. Una de las funciones principales de la aplicación es interceptar mensajes SMS y leer el historial de llamadas. Más de 2200 usuarios se han visto afectados por esta muestra.
5. **MobileTracker.c** incluye funciones como interceptar mensajes de las redes sociales más populares y controlar el dispositivo afectado de forma remota. Más de 2100 usuarios se han visto afectados por esta muestra.
6. **PhoneSpy** también es conocido como Spy Phone o Spapp Monitoring. Esta aplicación contiene muchas funciones para espiar en todas las aplicaciones conocidas de mensajería instantánea y redes sociales.
7. **Agent.hb** es otra versión de MobileTracker. Como en la versión original, ofrece numerosas funciones.
8. **Cerberus.b** es una muestra distinta de la misma familia que Cerberus.a.
9. **Reptilic.a** es un stalkerware que incluye muchas funciones, como el control de redes sociales, grabaciones de llamadas y el control del historial del navegador.
10. **SecretCam.**a es un software de supervisión de la cámara, es decir, puede grabar vídeos secretamente con la cámara frontal o trasera del dispositivo afectado.

Geografía de los usuarios afectados

El stalkerware es un fenómeno mundial que afecta a países independientemente de su tamaño, sociedad o cultura. Al analizar cuáles eran los diez países más afectados del mundo en 2020, Kaspersky constató que prácticamente eran los mismos países los que seguían viéndose afectados, siendo Rusia el número uno. Además, se observa un aumento de la actividad de stalkerware en Brasil y EE. UU. en 2020 en comparación con 2019. Sin embargo, detectamos menos incidentes en India, que ha caído varios puestos en la clasificación. También hemos detectado un número elevado de incidentes en México, que ha subido dos puestos en la clasificación.

	País	Usuarios afectados
1	Rusia	12389
2	Brasil	6523
3	Estados Unidos	4745
4	India	4627
5	México	1570
6	Alemania	1547
7	Irán	1345
8	Italia	1144
9	Reino Unido	1009
10	Arabia Saudí	968

Tabla 4: Los diez países más afectados por stalkerware en 2020 (a nivel mundial)

En Europa, Alemania, Italia y el Reino Unido son los tres países más afectados en ese orden. Les sigue Francia en cuarto lugar y España en quinto lugar.

	País	Usuarios afectados
1	Alemania	1547
2	Italia	1144
3	Reino Unido	1009
4	Francia	904
5	España	873
6	Polonia	444
7	Países Bajos	321
8	Rumanía	222
9	Bélgica	180
10	Austria	153

Tabla 5: Los diez países más afectados por stalkerware en 2020 (Europa)

Cómo comprobar si un dispositivo móvil tiene stalkerware instalado

Es difícil para un usuario común saber si tiene stalkerware instalado en sus dispositivos. Normalmente, este tipo de software permanece oculto: el icono de la aplicación de stalkerware no aparece en la pantalla de inicio ni en el menú del móvil e incluso se eliminan rastros de acciones que se han llevado a cabo. Sin embargo, puede delatarse y desvelar algunas señales de advertencia. Algunas de las más importantes son:

- Vigile si la batería se le acaba demasiado rápido, si el teléfono se sobrecalienta con frecuencia o hay un aumento del tráfico de datos móviles.
- Realice análisis antivirus con frecuencia en su dispositivo Android: si la solución de seguridad informática detecta stalkerware, **no se apresure a eliminarla, porque el agresor podría darse cuenta**. Organice un plan de seguridad y póngase en contacto con alguna organización local de asistencia.
- Compruebe el historial del navegador: para descargar el stalkerware, el agresor tiene que visitar algunas páginas web que el usuario afectado no conoce. También puede ser que no vea el historial porque el agresor lo haya borrado.
- Compruebe los ajustes de «fuentes desconocidas»: si las «fuentes desconocidas» están activadas en su dispositivo, puede que sea una señal de que se ha instalado software no deseado de fuentes de terceros.
- Compruebe los permisos de las aplicaciones instaladas: puede que la aplicación de stalkerware esté oculta con otro nombre y tenga acceso de forma sospechosa a mensajes, registros de llamadas, ubicación y otra actividad personal.

Sin embargo, también es importante entender que las señales o los síntomas de advertencia no son necesariamente una prueba de que se ha instalado stalkerware en un dispositivo.

En el contexto de la violencia doméstica y las relaciones de abuso, puede ser difícil o incluso imposible impedir que el agresor acceda al teléfono.

Cómo minimizar el riesgo

Hay algunos consejos que pueden ayudarle a aumentar su seguridad digital:

- Nunca preste su teléfono a nadie sin ver lo que hace con él ni lo deje desbloqueado.*
- Use una contraseña compleja para bloquear la pantalla y cambie las contraseñas con frecuencia.
- No le diga su contraseña a nadie, ni siquiera a su pareja, miembros de su familia ni amigos cercanos.*
- Realice comprobaciones frecuentes en su teléfono: elimine aplicaciones que no usa y revise los permisos concedidos a cada aplicación.
- Desactive la opción de instalación de aplicaciones de terceros en dispositivos Android.
- Proteja sus dispositivos Android con una solución de seguridad informática, como Kaspersky Internet Security para Android (gratuita), que detecta stalkerware y envía advertencias.

* En el contexto de la violencia doméstica y las relaciones de abuso, puede ser difícil o incluso imposible impedir que el agresor acceda al teléfono.

Actividades y contribución de Kaspersky para acabar con la ciberviolencia

Kasperksy trabaja continuamente para acabar con el uso de la ciberviolencia y el stalkerware, como empresa individual y en colaboración con otros socios. En 2019, creamos una alerta especial que avisa a los usuarios si se instala algún stalkerware en sus teléfonos. En el mismo año, junto con otros nueve miembros fundadores, creamos la Coalición contra Stalkerware. En 2020 creamos TinyCheck, una herramienta gratuita para detectar stalkerware en dispositivos móviles, concretamente para organizaciones que trabajan con víctimas de violencia doméstica. Puede encontrar TinyCheck en https://github.com/KasperskyLab/TinyCheck. Desde 2021, somos uno de los cinco socios que forman parte de un proyecto de la UE que pretende confrontar la violencia de género en Internet y el stalkerware (DeStalk). La Comisión Europea ha decidido apoyar este proyecto con su Programa de Derechos, Igualdad y Ciudadanía.

Acerca de la Coalición contra Stalkerware

La Coalición contra Stalkerware (CAS o Coalición) es un grupo que se centra en abordar los problemas de abuso y acoso derivados de la creación y el uso de stalkerware. Creada en noviembre de 2019, la Coalición contra Stalkerware sumó 26 socios en su primer año. Entre ellos, se incluyen socios fundadores: Avira, Electronic Frontier Foundation, European Network for the Work with Perpetrators of Domestic Violence (WWP EN), G DATA Cyber Defense, Kaspersky, Malwarebytes, National Network to End Domestic Violence, NortonLifeLock, Operation Safe Escape y WEISSER RING. La Coalición pretende reunir a una gran diversidad de organizaciones con el fin de abordar de forma activa el comportamiento delictivo que se lleva a cabo mediante stalkerware y generar conciencia sobre este importante asunto. Debido a su elevada importancia en el ámbito social para usuarios de todo el mundo y a las nuevas variantes de stalkerware que aparecen regularmente, la Coalición contra Stalkerware está abierta a nuevos socios y siempre busca cooperación. Para obtener más información sobre la Coalición contra Stalkerware, visite su sitio web oficial: https://stopstalkerware.org/es.