El estado del **stalkerware** en 2019

COALITION AGAINST STALKERWARE

kaspersky

COALITION AGAINST
STALKERWARE

Coalición contra el stalkerware

La Coalición contra el Stalkerware -"Coalition against Stalkerware"- es un nuevo grupo de trabajo mundial que reúne a expertos en ciberseguridad y a organizaciones de apoyo a víctimas para ayudar a los afectados.

Diez organizaciones (Avira, Electronic Frontier Foundation, European Network for the Work with Perpetrators of Domestic Violence, G DATA CyberDefense, Kaspersky, Malwarebytes, National Network to End Domestic Violence, NortonLifeLock, Operation Safe Escape y WEISSER RING) han lanzado en noviembre de 2019 la iniciativa mundial llamada "Coalition Against Stalkerware "para proteger a los usuarios contra el llamado stalkerware.

La coalición se formó para facilitar la comunicación entre la comunidad de ciberseguridad y aquellas organizaciones que trabajan para combatir la violencia de género. El portal online www.stopstalkerware.org facilita la transmisión de información entre sus miembros, elaborar procedimientos recomendados para el desarrollo de software ético y educar al público sobre los peligros del stalkerware.

El proyecto surge como una iniciativa no comercial destinada a reunir bajo el mismo paraguas a organizaciones sin ánimo de lucro, a la industria y a otras áreas y sectores de interés como fuerzas de seguridad. Dada su gran relevancia social en todo el mundo, y a las nuevas variantes de stalkerware que se desarrollan a diario, la Coalición contra el Stalkerware lanza un llamamiento para unirse e invita a la cooperación.

Para obtener más información, visite www.stopstalkerware.org

Los socios fundadores hablan sobre la importancia de **trabajar juntos contra el stalkerware**:

COALITION AGAINST STALKERWARE

Alexander Vukcevic,
Director Protection Labs
Avira

"En los últimos años, el software de monitorización ha evolucionado rápidamente, se han incorporado funciones avanzadas de vigilancia y la finalidad de la actividad de rastreo ha cambiado de manera fundamental. El continuo aumento del uso de dispositivos móviles, junto con la falta de legislación para su mitigación , hace que estas herramientas sean accesibles para que las personas espíen a sus cónyuges, familiares o amigos. En Avira, reconocemos que se trata de una nueva categoría de amenaza e invitamos a las empresas de seguridad informática y a las organizaciones que trabajan contra la violencia doméstica a unir fuerzas, compartir información y trabajar juntas para detener estas violaciones de privacidad".

Eva Galperin,
Directora de Ciberseguridad,
Electronic Frontier Foundation

"El stalkerware, que se utiliza para espiar teléfonos y equipos en situaciones de acoso o abuso doméstico, representa un problema muy grave que suele ir acompañado de otras formas de abuso, incluso la violencia física. La omnipresencia del stalkerware es un problema complejo y necesitamos a los actores de todos los sectores de la sociedad para combatirlo con eficacia".

Anna McKenzie,
Responsable de Comunicación,
European Network for the Work with Perpetrators of Domestic Violence (WWP EN)

"Los estudios demuestran que el 70% de las mujeres víctimas de ciberacoso también sufrió al menos una forma de violencia física osexual por parte de su pareja. Debemos impedir que estos acosadores utilicen los teléfonos para acosar y hacerlos responsables de su violencia. La Coalición contra el Stalkerware nos permite aportar a las empresas de seguridad informática nuestros conocimientos sobre violencia de género para trabajar juntos en la erradicación de la violencia perpetrada a través de nuevas tecnologías contra mujeres y niñas".

Hauke Gierow,
Portavoz,
G DATA CyberDefense

"Colocar un spyware en el teléfono de una pareja constituye una violación de los derechos humanos fundamentales. Estamos dispuestos a combatir este comportamiento y a proteger a las víctimas y supervivientes de estos comportamientos abusivos, que en su mayoría son mujeres. En G DATA Cyber Defense, estamos comprometidos a educar mejor a los usuarios sobre los posibles riesgos y a trabajar con organizaciones de víctimas para abordar también las cuestiones no técnicas que estén asociadas con el stalkerware".

Vyacheslav Zakorzhevsky,
Jefe del equipo de antimalware,
Kaspersky

"Es importante que los proveedores de ciberseguridad y las organizaciones de defensa y apoyo a las víctimas trabajen juntas para combatir este problema. La industria de la seguridad informática contribuye al mejorar la detección del stalkerware y notificar a los usuarios esta amenaza. Por su parte, las organizaciones trabajan directamente con víctimas de violencia de género, conocen su sufrimiento y puntos vulnerables, y pueden guiar nuestro trabajo. Por lo tanto, si trabajamos juntos codo con codo, podremos ayudar a las víctomas mediante la experiencia técnica y el desarrollo de funcionalidades".

David Ruiz,
Escritor de privacidad online,
Malwarebytes Labs

"Durante años, en Malwarebytes hemos detectado y advertido a los usuarios sobre las capacidades potencialmente peligrosas del stalkerware, una amenaza invasiva que puede robar a las personas sus expectativas y su derecho a la privacidad. De la misma forma que el abuso que permite, el stalkerware también se propaga lejos de la mirada pública y aísla a sus víctimas y supervivientes, que son ignorados y no reciben ayuda. El próximo paso para detener esta amenaza digital es organizarnos y luchar junto a la coalición contra el stalkerware. Se trata de un enfoque colaborativo guiado por la promesa de permitir el uso seguro de la tecnología para todos y en todo lugar".

Erica Olsen,
Directora de Safety Net Project,
National Network to End Domestic Violence

"Al estar diseñado para funcionar completamente en modo oculto y sin notificar de forma permanente al dueño del dispositivo, el stalkerware ofrece a los abusadores, acosadores y otros perpetradores una herramienta eficaz para cometer actos de acoso, monitorización, engaño y abuso. Este tipo de abuso puede ser aterrador y traumático, y plantea graves problemas de seguridad y privacidad. La creación de esta coalición representa un avance para abordar este problema".

Kevin Roundy,
Director de Investigación,
NortonLifeLock

"En NortonLifeLock, nuestros expertos en investigación han estado trabajando arduamente durante más de 12 años para arrebatarles el stalkerware a los abusadores y les han brindado a las víctimas y posibles víctimas herramientas para que se protejan y vivan una vida libre de acoso, violencia y ataques. Nos enorgullece ser miembros fundadores de la Coalición contra el Stalkerware para compartir nuestros conocimientos y unir fuerzas en la lucha contra el abuso".

Wilson "Chilly" Hightower,
Head of Intake
Operation Safe Escape

"La maliciosa existencia del stalkerware solo sirve para vulnerar, dañar e infundir una sensación constante de miedo y ansiedad en muchos de nuestros clientes. Representa una amenaza existencial y activa para la seguridad y la privacidad de todos. A medida que nuestras vidas se vuelven más dependientes de la tecnología, la amenaza que ya representa el stalkerware aumenta significativamente. Ahora resulta más importante que nunca adelantarnos a esta amenaza para quitarles el poder a los posibles abusadores, acosadores y otras entidades maliciosas. En Operation Safe Escape, nos sentimos muy orgullosos de ser parte de este esfuerzo para restaurar la privacidad y el sentimiento de seguridad de nuestros clientes y las personas de todo el mundo".

Horst Hinger,
Subdirector General,
WEISSER RING

"Como organización sin ánimo de lucro, sabemos que la tecnología facilita el acceso de los abusadores a los datos personales de sus víctimas. Las víctimas no suelen pedir ayudar porque se sienten avergonzadas. En WEISSER RING, el acoso constituye un problema de creciente importancia en nuestra labor de ayuda a las víctimas. En 2018, asistimos en 1.019 casos de acoso, que representó casi un tres por ciento más que el año anterior. Según las estadísticas de delitos de la policía alemana, en 2018 hubo en total casi 19.000 casos de acoso, 500 más que el año anterior, lo que también representa un claro incremento. En consecuencia, hemos desarrollado la aplicación NO STALK junto con WEISSER RING Foundation para brindar a las víctimas una herramienta eficaz para registrar el acoso en forma de evidencia".

Principales hallazgos, actualización: abril de 2020

A nivel mundial, el número de usuarios con stalkware instalado en sus dispositivos aumentó un 67% en tan solo un año

Esta sección ofrece una actualización con las cifras para todo el año 2019 en comparación con 2018. Debido a la fecha de publicación, la parte restante del informe incluye datos de enero a agosto de 2019.

- A finales de 2019, el número de nuestros usuarios móviles víctima de stalkware aumentó en un 67%: en 2018, 40,386 usuarios se enfrentaron a este tipo de ataque, mientras que en 2019 la cifra ascendió a 67,500
- El número de ataques se duplicó durante la segunda mitad de 2019 en comparación con el primer semestre del año. En enero de 2019, 4,483 usuarios móviles de Kaspersky cayeron en la trampa; en septiembre, la cifra ascendió a 9,546 y, en diciembre del mismo año, se registraron 11,052 casos
- Rusia, Brasil, India y Estados Unidos son las regiones del mundo más propensas a sufrir ataques de stalkware y constituyeron, respectivamente, el 23.4%, el 9.4%, el 9% y el 5.6% de los usuarios afectados en 2019
- En Europa, Alemania (3.1 %), Italia (2.4 %) y Francia (1.8 %) son los tres países más afectados

Resumen

El "stalkerware" es una herramienta que permite al acosador controlar a su víctima sin su consentimiento

Introducción y metodología

Hace seis meses, creamos una alerta especial para notificar a los usuarios acerca de los productos comerciales de spyware (stalkerware) que tenían instalados en sus teléfonos. El presente informe analiza el uso del stalkerware y la cantidad de usuarios afectados por este software en los primeros ocho meses de 2019.

En los últimos años, la tecnología de vigilancia ha evolucionado con rapidez y su propósito fundamental ha cambiado de forma drástica. El auge de Internet y el incremento del uso de dispositivos móviles han dado lugar a un tipo de software de vigilancia conocido como stalkerware y que gana popularidad. El software permite que los usuarios espíen a otras personas, por ejemplo, permite monitorizar los mensajes, acceder a la información de llamadas y las ubicaciones GPS, de forma oculta. Suele utilizarse para violar la privacidad de parejas actuales o anteriores, e incluso de extraños. Y esto puede hacerse simplemente instalando de forma manual una aplicación en el teléfono inteligente o tablet de la víctima elegida. Una vez instalado, el acosador obtiene acceso a una serie de datos personales, a pesar de estar lejos de la víctima. Hay que hacer una importante diferencia con el software de control parental. Mientras que las aplicaciones de control parental buscan restringir el acceso a contenidos inapropiados o peligrosos y notifican constantemente al usuario sobre sus solicitudes, el stalkerware se encarga de otorgar al acosador una herramienta de vigilancia para espiar a la víctima sin su consentimiento.

La gran mayoría de las aplicaciones de stalkerware no se encuentran disponibles en tiendas oficiales de aplicaciones, como Google Play, y su instalación requiere acceso a un sitio web específico y al dispositivo de la víctima. Personas malintencionadas pueden usarlo para controlar los correos electrónicos de sus empleados, rastrear los movimientos de sus hijos e incluso espiar a su pareja. Estos usos pueden causar hostigamiento, vigilancia sin consentimiento, acoso e incluso violencia doméstica. Sin embargo, las leyes que actualmente regulan el uso del stalkerware no son lo suficientemente firmes como para impedir que los acosadores se aprovechen y abusen de otras personas.

Los datos en este informe se extrajeron de las estadísticas totales de amenazas obtenidas de Kaspersky Security Network, con el propósito de medir la frecuencia y la cantidad de usuarios que encontraron stalkerware en los primeros ocho meses de 2019 en comparación con los datos obtenidos el año pasado. La infraestructura de Kaspersky Security Network está diseñada para procesar los flujos de datos relacionados con la seguridad cibernética de millones de voluntarios de todo el mundo. En este informe, investigamos por qué se usa el stalkerware y dónde se implementa más.

Principales hallazgos

En solo un año, el número de usuarios afectados por Stalkerware aumentó un 35% a nivel global

- De enero a agosto de 2019, hubo más de 518.223 casos en todo el mundo en los que nuestras tecnologías de protección registraron la presencia de stalkerware en los dispositivos de usuarios o detectaron un intento de instalación. Esto representa un aumento del 373 % con respecto al mismo período de 2018.
- En los primeros ocho meses de 2019, 37.532 usuarios detectaron stalkerware al menos una vez; lo que supone un aumento del 35 % en comparación con el mismo período de 2018 (27.798 usuarios).
- La cifra de usuarios víctimas de lo que se conoce como troyanos espía fue de 26.620 en los primeros ocho meses de 2019, una cifra relativamente pequeña en relación a los usuarios que detectaron stalkerware.
- La Federación Rusa es la región donde más stalkerware se detectó a nivel mundial, con el 25,6 % de usuarios potencialmente afectados en los primeros ocho meses de 2019. En el segundo puesto, se encuentra India con el 10,6 % de usuarios afectados y, en el tercer puesto, Brasil (10,4 %). Los Estados Unidos se ubican en el cuarto puesto con el 7,1 %
- En cuanto a Europa, Alemania, Italia y Reino Unido ocupan los tres primeros puestos respectivamente.

Aumento del problema del stalkerware

Durante este año, se ha producido un fuerte aumento en el número de detecciones de stalkerware en dispositivos Android protegidos por los productos de Kaspersky. Una de las razones de este aumento podría ser la mejora en la detección de stalkerware a través de soluciones de seguridad.

En abril, Kaspersky lanzó una función en su app de seguridad de Android: **Privacy Alert** (Alerta de privacidad), que alerta a los usuarios si su dispositivo tiene instalado un software que pueda utilizarse para acosar.

Desde entonces, el número de detecciones ha aumentado de forma continua. Por ejemplo, en marzo de 2019, el número de usuarios que detectó stalkerware fue de 4.315 en comparación con los 7.075 en abril. Esto representa un aumento del 64 % en solo un mes. Esta cifra subió a 9.251 durante agosto, un 94 % más que el mes anterior a lanzar la función.

Por lo general, estos programas de vigilancia suelen utilizarse para espiar a conocidos, amigos, familiares o parejas, y tienen una gran demanda. Por un precio relativamente bajo, a veces poco más de 6 euros al mes, estas aplicaciones se mantienen ocultas mientras informan a los acosadores sobre la actividad del dispositivo, como la ubicación, el historial de navegación, los mensajes de texto, las conversaciones en las redes sociales, etc. Algunas de estas aplicaciones incluso pueden grabar voz y vídeo.

Para examinar aun más la magnitud del problema de stalkerware, en Kaspersky se ha analizado la actividad de los últimos ocho meses. Entre enero y agosto de 2019, 37.533 usuarios detectaron stalkerware al menos una vez en sus dispositivos. Esto supone un aumento del 35 % con respecto al mismo período del año anterior.

En general, hubo 518.223 casos en los que los productos de Kaspersky registraron la presencia de stalkerware en los dispositivos de usuarios o detectaron un intento de instalación entre enero y agosto de 2019, un impactante aumento del 373 % en comparación con el mismo período de 2018.

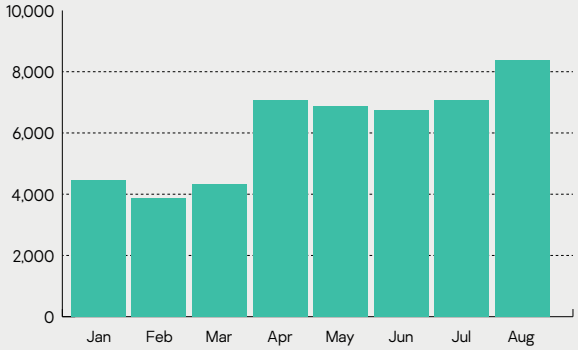


Fig. 1 Número de usuarios que detectaron stalkerware entre enero y agosto de 2019

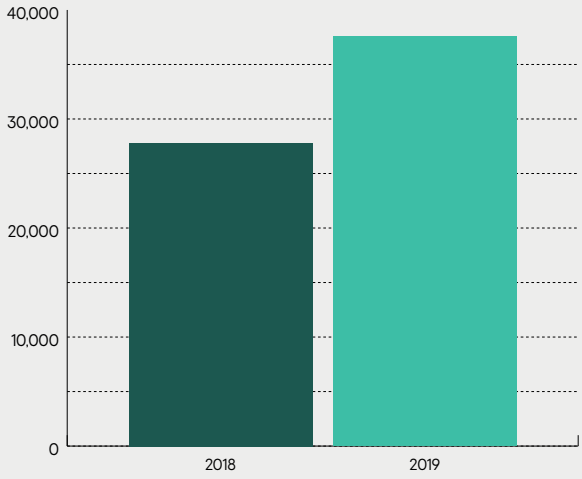


Fig. 2 Usuarios objetivo de stalkerware, 2018 vs. 2019

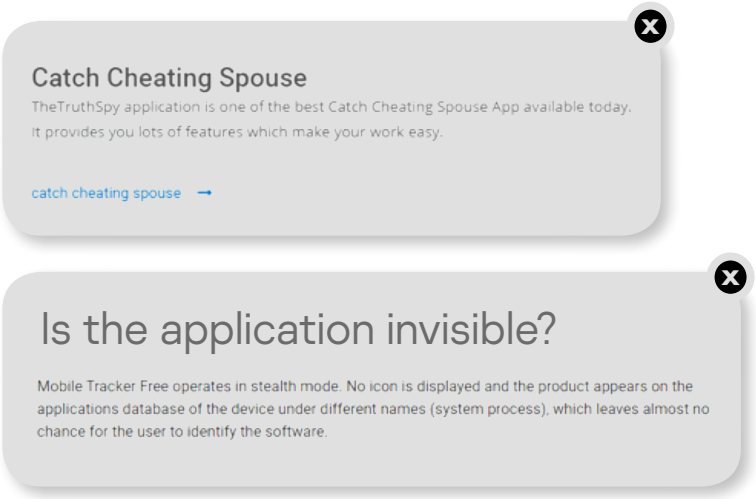


Fig. 3 Capturas de pantalla del sitio web oficial de Mobile Tracker Free

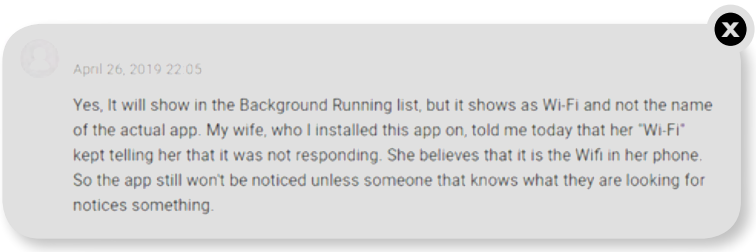


Fig. 4 Captura de pantalla del sitio web oficial de TheTruthSpy

Un tercero podría acceder a las fotos almacenadas en el teléfono de la víctima e incluso a la cámara en tiempo real, así como al historial de navegación, los archivos, el calendario o los contactos

Ejemplos de software utilizados para el acoso

La familia de stalkerware más prolífica en 2019 se identificó como Monitor.AndroidOS.MobileTracker.a y afectó a 6.559 usuarios. En segundo lugar, Monitor.AndroidOS.Cerberus.a fue detectado en los dispositivos de 4.370 usuarios, seguido de cerca por Monitor.AndroidOS.Nidb.a (4.047).

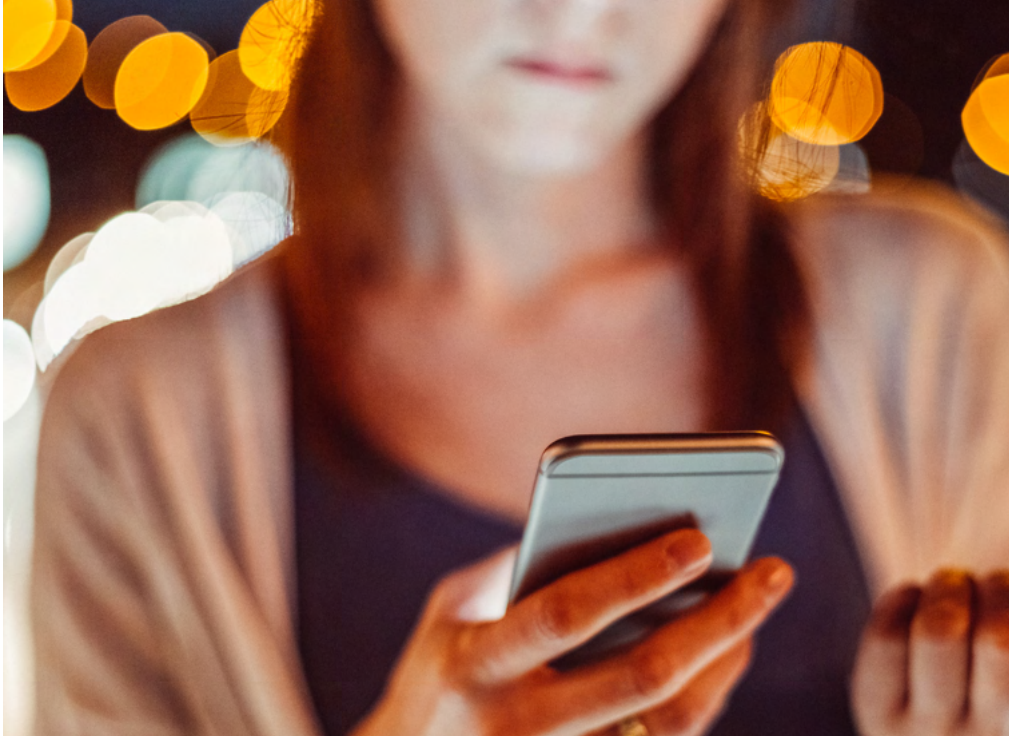
Si se comparan con los resultados del 2018, las dos primeras difieren del año pasado. Monitor.AndroidOS.Nidb.a y Monitor.AndroidOS.PhoneSpy.b se encontraron con mayor frecuencia en los dispositivos de usuarios durante 2018 y alcanzaron cifras de 4.427 y 2.819, respectivamente. Monitor.AndroidOS.XoloSale.a fue el tercer stalkerware más común y afectó a 1.946 usuarios.

En nuestro sistema de clasificación interno, se utiliza un registro de Monitor.AndroidOS.MobileTracker.a para identificar una aplicación de Mobile Tracker Free, una herramienta para rastrear la actividad de niños o empleados. De hecho, la aplicación permite el rastreo de la ubicación del usuario, su correspondencia SMS y aplicaciones de mensajería (WhatsApp, Hangouts, Skype, Facebook Messenger, Viber, Telegram, etc.), así como sus llamadas. También permite que un tercero acceda a las fotos de la víctima desde el teléfono y la cámara en tiempo real, junto con el historial de navegación, los archivos almacenados en el dispositivo, el calendario y la lista de contactos. Asimismo, la aplicación permite controlar el dispositivo de forma remota. Además de todo esto, existe la posibilidad de trabajar en modo oculto bajo el disfraz de aplicaciones del sistema.

La siguiente aplicación, Cerberus (Monitor.AndroidOS.Cerberus.a), se cataloga como una aplicación antirrobo. Sin embargo, también permite que los acosadores trabajen en modo "oculto" e impidan su eliminación. Entre otras funciones, permite rastrear la ubicación del dispositivo, tomar fotografías desde la cámara y capturas de pantalla, así como grabar audio desde el micrófono.

La que se ubica en tercer lugar, Monitor.AndroidOS.Nidb.a, en realidad forma parte de un grupo de aplicaciones similares llamado iSpyoo/TheTruthSpy/Copy9. A diferencia de las dos aplicaciones anteriores, algunos representantes de este grupo se anuncian públicamente como un medio para espiar a la pareja e incluso escriben artículos sobre ello.

Si bien el conjunto de funcionalidades es bastante estándar en estos programas, no deja de ser impresionante: rastreo de sitios web, interceptación de correspondencia en aplicaciones de mensajería y SMS, rastreo de llamadas e historial de navegación. Como muchas otras aplicaciones similares, requieren los permisos de superusuario (derechos de administración) para controlar algunas funciones. Pueden trabajar en modo "oculto" y los nombres que se encuentran en la lista de aplicaciones instaladas imitan los procesos del sistema.



¿Dónde se encuentra el stalkerware?

Según demuestra el amplio abanico de regiones donde se producen la mayoría de los ataques, existe un mercado mundial de stalkerware y spyware legales. Los 10 países con el mayor porcentaje de usuarios atacados por stalkerware no poseen similitudes geopolíticas ni se encuentran cerca.

1. Federación Rusa – **25.61%**
2. India – **10.56%**
3. Brasil– **10.39%**
4. Estados Unidos – **7.11%**
5. Alemania – **3.55%**
6. Italia – **2.65%**
6. Méjico – **2.10%**
8. Reino Unido – **1.95%**
9. Francia– **1.76%**
10. Irán – **1.68%**

Otros – **32.65%**

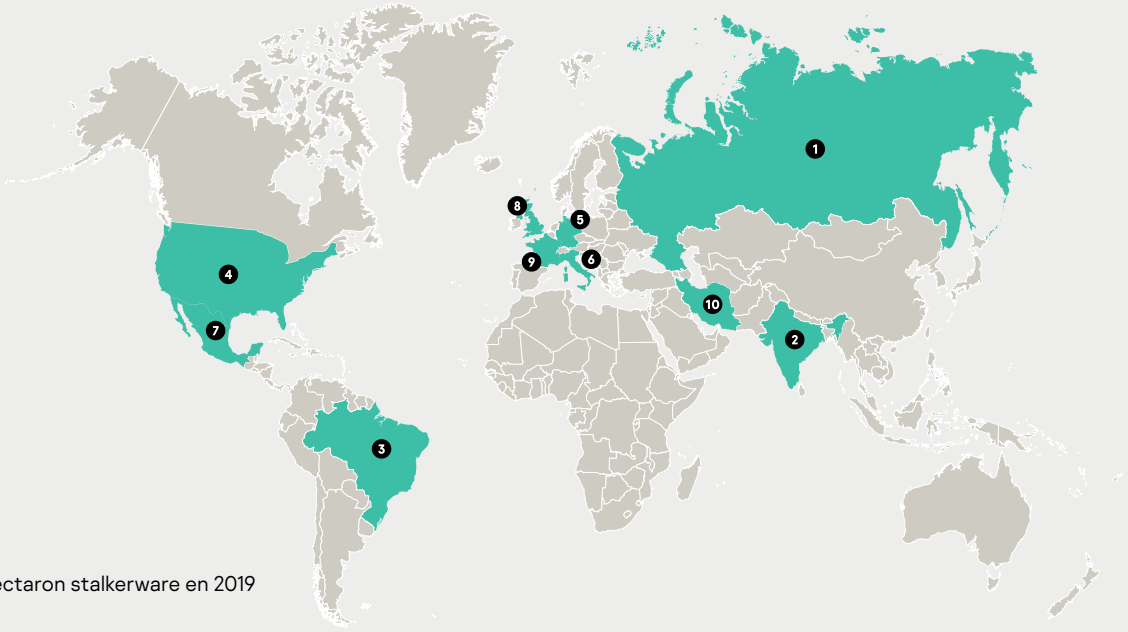


Fig. 5 Geografía de usuarios que detectaron stalkerware en 2019

El 85 % de las personas que trabajan en centros de asistencia a víctimas de violencia doméstica, indicaron haber tratado casos en los que la víctima fue rastreada a través de GPS

El informe de Kaspersky muestra que la región con mayor actividad de stalkerware es Rusia. En India, la actividad persistente desde enero hasta agosto ha provocado que el país sea la segunda región más importante en cuanto a incidentes por stalkerware, con el 10,56 % de usuarios afectados.

Brasil representó el 10,39 % de usuarios atacados en 2019, mientras que Estados Unidos es la cuarta región (7,11 %). EE.UU cuenta con grupos de apoyo para concienciar sobre los peligros del stalkerware y llevan a cabo diversas investigaciones. La organización National Public Radio realizó encuestas en 72 refugios para víctimas de violencia doméstica y el 85 % de las personas que trabajan allí indicaron haber ayudado a víctimas de acosadores que las rastreaban por GPS. Casi tres cuartos (71 %) de los agresores controlaban las actividades en el ordenador de sus víctimas; mientras que el 54 % rastreba los teléfonos móviles con stalkerware.

El quinto país de la lista en 2019 fue Alemania con el 3,55 %.

Stalkerware en el panorama de las ciberamenazas

Más de 37.000 usuarios se vieron afectados por el stalkerware en 2019; mientras que en 2018 se registraron 27.000

Al comparar el stalkerware y el spyware con el resto de ataques a los que se enfrentan los usuarios móviles (como adware, riskware y malware), estos suponen una buena parte de los programas maliciosos catalogados como "no virus". En los primeros ocho meses de 2019, Kaspersky detectó 2.350.862 usuarios atacados con amenazas potencialmente no deseadas y solo el 1,60 % de ellas estaban relacionadas con stalkerware. Sin embargo, a diferencia de la mayoría de las potenciales amenazas masivas (como adware), el stalkerware requiere de un acosador, una persona concreta, para actuar y llevar a cabo su operación. El acosador elige a una víctima en concreto, con un propósito específico. Por lo tanto, si bien los números son más bajos, el stalkerware requiere de mayor esfuerzo para llegar y afectar a su víctima y conlleva una intención de abuso detrás de cada una de estas actividades.

A fin de obtener un panorama general de la dinámica de desarrollo de stalkerware, comparamos el stalkerware con el malware de vigilancia ilegal para PC que detectamos como espías troyanos. Los resultados demuestran que el uso de spyware ilegal está en declive; mientras que el stalkerware se encuentra en fase de gran crecimiento.

Nuestro análisis de los primeros ocho meses de 2019 demuestra que la cantidad de usuarios que detectaron stalkerware es superior a la cantidad de ataques de espías troyanos. Mientras que en 2018 se registraron más de 43.000 objetivos de spyware en comparación con alrededor de 28.000 objetivos de stalkerware, en 2019 la situación ha dado un giro. La cantidad de usuarios que detectaron stalkerware creció un 35 % y llegó a más de 37.000 afectados; mientras que las herramientas de spyware afectaron a 26.620 usuarios.

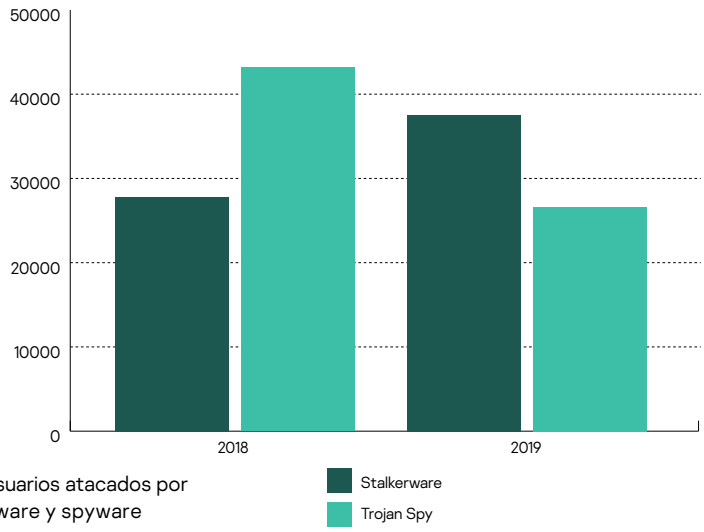


Fig. 6 Usuarios atacados por stalkerware y spyware

Durante estos meses de 2019, los incidentes relacionados con el stalkerware detectados por los productos de Kaspersky ha sufrido un aumento importante dentro del total de amenazas. Entre enero y agosto del año pasado, el stalkerware representó el 1,01 % del número total de usuarios (2.740.023) que se enfrentó a algún tipo de software potencialmente peligroso (adware y otros de la categoría "no-virus"). El stalkerware está creciendo en popularidad mientras que los ataques por malware más tradicionales son menos prolíficos que hace 12 meses.

Conclusiones y recomendaciones

Es evidente que el stalkerware está en auge y está cobrando mayor importancia en el panorama de la ciberseguridad. Si nos fijamos en las fluctuaciones interanuales del número total de ataques de riskware, adware y spyware, el porcentaje de incidentes relacionados con el stalkerware sigue aumentando. Descubrir el papel de estos acosadores en el panorama de las ciberamenazas puede llevar tiempo, pero cada vez se registran más incidentes. Desde que Kaspersky lanzó su solución para notificar a los usuarios si sus dispositivos tenían instalado stalkerware en abril de 2019, el número de detecciones ha aumentado.

También parece haber cierta consistencia en cuanto a los países con mayor probabilidad de sufrir incidentes por stalkerware, con Rusia, India, Estados Unidos y Alemania dentro de los más destacados en los últimos dos años.

La buena noticia para los usuarios es que se están aplicando soluciones efectivas para que puedan protegerse. Empresas de seguridad informática y organizaciones que trabajan con víctimas de abuso doméstico deben unir fuerzas para que las empresas de ciberseguridad puedan responder mejor a los casos de stalkerware. Estas iniciativas ayudarán a las víctimas a través de la tecnología y la experiencia. Con este fin, Kaspersky ha sumado fuerzas con otras organizaciones y ha creado la Coalición contra el Stalkerware (Coalition Against Stalkerware).

Creemos que toda persona tiene derecho a la protección de su privacidad. Compartimos nuestra experiencia en ciberseguridad, trabajamos y colaboramos estrechamente con organizaciones internacionales y fuerzas de seguridad para combatir a los cibercriminales. Desarrollamos tecnologías, soluciones y servicios para ayudarte a protegerte de las amenazas cibernéticas.

Acerca de Kaspersky

Kaspersky es una compañía global de ciberseguridad fundada en 1997. La profunda experiencia de Kaspersky en inteligencia de amenazas y seguridad se está continuamente transformando en innovadoras soluciones y servicios de seguridad para proteger a empresas, infraestructuras críticas, gobiernos y consumidores en todo el mundo. El extenso portfolio de productos de seguridad de la empresa incluye su reputada solución de protección de endpoints, junto con una serie de soluciones y servicios de seguridad especializados para combatir las sofisticadas y cambiantes amenazas digitales. Más de 400 millones de usuarios son protegidos por las tecnologías de Kaspersky y ayudamos a 270.000 clientes corporativos a proteger lo que más les importa.

www.kaspersky.es

www.securelist.com

kaspersky