Programas espía (spyware) y de acoso: vigilancia de computadoras y seguridad para sobrevivientes

¿Qué son los programas espía (spyware) y de acoso?

Los programa espía (spyware) y de acoso (stalkerware) son herramientas, es decir: aplicaciones, programas de software y dispositivos que permiten que una persona no autorizada (como un/a agresor/a) pueda controlar y registrar secretamente la información de su computadora. El término “stalkerware” (programa de acoso) es una expresión reciente que refiere al uso indebido invasivo, intrusivo y peligroso de estas herramientas.

Un programa espía (spyware) puede rastrear casi todo lo que usted haga en su computadora; esto incluye cada cosa que haya escrito, sitio web que haya visitado, mensaje enviado o recibido y cada documento que haya abierto. Algunos programa espía (spyware) también permiten que la persona que lo haya instalado encienda la cámara web o el micrófono, que tome fotos de pantalla, que haga hablar a la computadora o le permita hacer ruidos, o que apague o reinicie la computadora. La persona agresora puede ver la actividad de su computadora o controlarla a distancia, normalmente mediante un panel en un sitio web o con una aplicación.

La mayoría de los programa espía (spyware) pueden ser instalados de forma remota enviando un correo electrónico o un mensaje con un archivo adjunto o un enlace. El programa espía (spyware) se instala automáticamente cuando hace clic en el enlace o cuando abre el adjunto. Algunos programa espía (spyware) pueden ser enviados mediante mensajería instantánea, juegos o cualquier otra estrategia para atraerlo/la a usted o a sus hijos/as a abrir el archivo adjunto o el enlace. Una vez instalado, el programa funciona de forma sigilosa, sin ninguna notificación o actividad característica y son difíciles de detectar o eliminar.

Mientras que la mayoría de los programa espía (spyware) se instalan como software, también existen programas espía con base en hardware denominados registradores de pulsaciones. Estos dispositivos de registro de pulsaciones pueden parecer una parte normal de la computadora, por ejemplo, un teclado especial con función de registro de pulsaciones o un dispositivo pequeño que se conecta al teclado de una computadora. Una vez conectado a la computadora, el dispositivo registra cada tecla presionada, lo cual puede incluir contraseñas, números de identificación personal (PIN) y sitios web visitados. Algunos dispositivos de hardware permiten espiar a distancia, mientras que otros requieren que el/la agresor/a acceda al dispositivo para obtener la información de la actividad de la computadora.

¿Cómo puedo saber si hay un programa espía (spyware) en mi computadora?

Puede resultar muy difícil encontrar un programa espía (spyware). En la mayoría de los casos, una computadora con un programa espía (spyware) instalado no sufrirá grandes cambios en la forma en la que opera (su computadora no será más lenta ni se congelará). Incluso sin que sucedan estas cosas, usted podría sospechar que su actividad está siendo registrada por el comportamiento sospechoso del/de la agresor/a. Confíe en sus instintos y busque señales. Si la persona abusiva sabe demasiado sobre su actividad en la computadora, o sabe cosas que usted solo hizo en su computadora o teléfono, es posible que su dispositivo tenga un programa espía (spyware).

Si se instaló un dispositivo de hardware, usted podría ver un componente adicional entre su computadora y el cable del teclado, o podría tener un nuevo mouse o teclado inesperadamente. En las computadoras portátiles, un dispositivo de hardware podría no ser tan notorio ya que estaría instalado dentro de la computadora, mediante el panel de acceso.

Responder a un programa espía (spyware)

La seguridad es lo primero. Antes de realizar alguna acción para encontrar o quitar el programa espía (spyware), es importante tener en cuenta la seguridad y la posibilidad de recolectar evidencia. Ya que muchos/as agresores/as utilizan programas espía (spyware) para vigilar y controlar a los/las sobrevivientes, la persona podría aumentar su maltrato o comportamiento abusivo si sospecha que el/la sobreviviente intenta eliminar el programa espía (spyware) y cortar su acceso. Antes de quitar el programa espía (spyware), piense en su seguridad y considere formas en las que podría protegerse a sí mismo/a, y consulte a un/a intercesor/a acerca de un plan de seguridad. Si necesita un/a intercesor/a, por favor llame a la plan de seguridad.

Recolectar evidencia. La policía o un/a experto/a en informática forense podría asisistirlo/a si quisiera preservar evidencia para una investigación criminal o para una acción civil. Las herramientas forenses podrían ser la única manera de determinar si hay un programa espía (spyware) en una computadora. Conozca más sobre Evidencia de Programa Espía (spyware).

Quitar un programa espía (spyware). Podría ser muy difícil eliminar un programa espía (spyware) una vez instalado en una computadora. Puede considerar una limpieza total y reconstrucción de la computadora, que empezaría por reinstalar el sistema operativo, aunque esto no le asegura una eliminación total. Otra opción es reemplazar el disco duro de la computadora u obtener una nueva computadora. Tenga cuidado de no copiar archivos o documentos de la computadora infectada en la nueva computadora, ya que podría reinstalar el programa espía (spyware) oculto en los archivos. Utilice un servicio de almacenamiento en la nube para guardar los documentos de la computadora infectada.

Utilizar dispositivos que no estén controlados. Si sospecha que hay un programa espía (spyware) en su dispositivo, recuerde que toda actividad, incluidos los chat en línea, correos electrónicos y búsquedas en internet, puede ser revelada al/a la agresor/a. Si puede, utilice un dispositivo seguro o computadora segura con el que la persona no haya tenido contacto físico ni remoto cuando busque información o pida ayuda. Un dispositivo seguro podría ser la computadora de una biblioteca pública o de un centro comunitario o el dispositivo de un/a amigo/a.

Actualizar las cuentas. Debido a que el programa espía (spyware) le habría dado acceso a la persona abusiva a su información de entrada, considere cambiar sus contraseñas en un dispositivo diferente y no volver a acceder a ciertas cuentas desde la computadora que cree que está controlada. También considere cambiar las contraseñas de cuentas importantes como las de un banco virtual, cuentas de redes sociales, etc. Lea más sobre Seguridad de las Contraseñas.

Prevenir el programa espía (spyware)

Considerar el acceso. Sospeche si un/a agresor/a quiere instalar un nuevo teclado, cable, programa, actualización o si "arregla" el teléfono o la computadora. Sobre todo si esto coincide con un aumento en el control o el acecho. Tenga cuidado con los regalos que el/la agresor/a le haga a usted o sus hijos, como nuevos teléfonos, computadoras, teclados o juegos.

Crear un usuario separado o cuentas de invitado. Usted puede crear cuentas de invitado o una cuenta de administrador que tenga ajustes que no permitan que se instalen aplicaciones ni software sin que ingrese el administrador. Esto puede prevenir que se instale un programa espía (spyware) o cualquier otro programa malicioso por accidente o si alguien más utiliza su computadora y abre un enlace o archivo.

Utilizar una protección antivirus o software *antispyware*. Instale programas antivirus o contra programas espía (spyware); asegúrese de que estén actualizados y configúrelos para que registren su computadora de forma periódica. Estos programas pueden ayudar a prevenir que se instalen programas espía (spyware), pero funcionan mejor antes de que su computadora esté comprometida. Además, antes de navegar en línea o hacer clic en un enlace, active el antivirus/software *antispyware* para tener más protección. (Tenga en cuenta que estos programa solo protegen contra software de programa espía (spyware) pero no protegen de dispositivos, como un teclado o un dispositivo registrador de pulsaciones).

¿No hay programas espía (spyware)?

Existen muchos otros métodos con los que una persona podría acceder a la información de su computadora sin instalar un programa espía (spyware). Si el/la agresor/a tiene acceso físico a la computadora, podría no necesitar instalar un programa espía (spyware), que normalmente se utiliza para el control a distancia.

La persona agresora también podría ingresar a cuentas de correo electrónico o redes sociales para saber lo que usted está haciendo. Se puede acceder a estas cuentas desde otro dispositivo si la persona agresora conoce el nombre de usuario/a o correo electrónico y la contraseña.

A veces, la explicación a que una persona agresora conozca mucho sobre lo que usted hace podría ser tan simple como que su familia o amigos/as compartan información sobre usted. Buscar patrones respecto de lo que sabe la persona y pensar dónde pudo haber obtenido esa información podría ayudar a limitar las posibilidades. Un/a intercesor/a podría ayudarle a descubrir lo que está sucediendo y a planificar sus próximos pasos.

 Financiado por la Oficina de Víctimas de Crímenes del Departamento de Justicia (OVW, DOJ, por sus siglas en inglés) de los Estados Unidos. Subvención n.º 2016-TA-AX-K069. Las opiniones, hallazgos, conclusiones o recomendaciones aquí expresados pertenecen a el/la autor/a y no necesariamente reflejan los puntos de vista del Departamento de Justicia (DOJ, por sus siglas en inglés).

Actualizamos nuestro material con frecuencia. Visite TechSafety.org para obtener la última versión de este y otros materiales.