Image not found or type unknown

www.juventudrebelde.cu

Image not found or type unknown

El uso de software espía ha crecido en medio de la pandemia Autor: Kaspersky Latinoamérica Publicado: 29/07/2020 | 08:47 pm

Stalkerware: la otra pandemia a la sombra del coronavirus

El uso de programas malignos para acosar a otros, especialmente entre parejas, ha crecido desde que el virus SARS-CoV-2 paralizó el mundo en marzo pasado

Publicado: Miércoles 29 julio 2020 | 09:06:14 pm.

Publicado por: Yurisander Guevara

John envió a su esposa un sencillo mensaje: «Te amo». Pero ella no solo lo recibió, sino que podía ver todas las fotos, escuchar todas las llamadas y saber todos los movimientos de su compañero de vida, gracias a un software espía que había instalado en el celular de John sin que este lo supiera.

Así lo relata la publicación Vice en un reportaje que utiliza a John —un policía que, irónicamente, fue afectado por el programa maligno PoliceSheriff, desarrollado por la compañía Retina X—, como motivo para alertar sobre el uso de *stalkerware*, término cuyo significado proviene de stalker, que no es más que acosador en idioma inglés.

De acuerdo con un reciente reporte de la compañía de seguridad Avast, dedicada a la producción de antivirus, el uso de *stalkerware* va en aumento, y se ha visto un incremento de al menos el 50 por ciento de equipos afectados por este tipo de software desde que se desató la pandemia del coronavirus SARS-CoV-2.

El reporte, publicado el pasado 8 de julio, indica que desde enero solo esa compañía antivirus protegió a más de 43 000 clientes de aplicaciones *stalkerware*, con un incremento, solo en Estados Unidos, del 62 por ciento en el mes de marzo. Otros países que registraron un mayor uso de *stalkerware* fueron India y Brasil, apunta el informe de Avast.

La situación ha sido llamada como «la pandemia sombría del coronavirus» por Phumzile Mlambo-Ngcuka, directora ejecutiva de ONU Mujeres.

Investigadores en Estados Unidos publicaron recientemente un estudio académico que examina el impacto de la crisis provocada por la COVID-19 en las llamadas a la policía por violencia doméstica. Según el informe, la pandemia y la respuesta de salud pública que la acompañó llevaron a un aumento del 10,2 por ciento en las llamadas de violencia doméstica.

El aumento en este tipo de incidentes comenzó antes de que se establecieran las órdenes oficiales de permanecer en el hogar, no es impulsado por ningún grupo demográfico en particular, pero parece ser mayor en hogares sin antecedentes de violencia doméstica, apunta el estudio.

Una mayor cantidad de dispositivos conectados y la disponibilidad de aplicaciones sigilosas o*stalkerware* constituyen una vía para que los abusadores ejerzan control sobre sus víctimas, las que no han podido abandonar el hogar debido a las medidas preventivas ante el nuevo coronavirus, comentó Erica Olsen, directora del proyecto Red de seguridad nacional para terminar con la violencia doméstica, una organización dedicada a crear un entorno social, político y económico en el que la violencia contra las mujeres no exista, según PR Newswire.

El *stalkerware* está diseñado para operar de forma invisible, sin notificar al usuario, lo que brinda a los acosadores una herramienta robusta e invasiva para perpetrar acoso, monitoreo, acecho y abuso, acotó Olsen.

Por lo pronto, Google anunció que eliminará los anuncios de*stalkerware* de sus plataformas de publicidad, ya que muchos de estos programas se presentan como destinados a un «control parental», aunque en realidad sus propósitos son bien oscuros.

Cómo funciona

La mayoría de los *stalkerwares* son programas que no están disponibles en las tiendas de aplicaciones oficiales, como Google Play. Afectan principalmente a dispositivos con sistema operativo Android, debido a que en estos es más fácil instalar una aplicación de forma manual. En los equipos con iOS, a no ser que estén «liberados» —lo que se conoce como *jailbreak*—, es imposible instalar un programa maligno de este tipo. También están presentes en los ordenadores con Windows o Mac OS.

Los que pretendan usar un *stalkerware* deberán obtener el programa de webs dedicadas a ello, y necesitan, además, acceso al dispositivo de su víctima.

Una vez instalado, el software espía es capaz de pasar desapercibido para el usuario: no envía notificación alguna ni deja un ícono de la aplicación visible.

Un *stalkerware* necesita de internet para funcionar. Transmite los datos del dispositivo afectado al servidor del acosador, el cual puede acceder virtualmente a casi todos los datos de su víctima.

Es muy común, según fuentes especializadas, que también se use el *stalkerware* a través de servidores de terceros. Esto significa que el perpetrador instalará su servidor de acoso en la nube, y allí serán enviados los datos de la víctima. En este caso, la gran pregunta es si el acosador no sería también acosado por quienes le proveen un servicio de almacenamiento remoto para que guarde intimidades y conversaciones personales. En la era de la información, los datos son oro.

De hecho, en YouTube es posible encontrar videos en los que se demuestra cómo un *stalkerware* recopila datos de la víctima y los envía a servidores externos desde el momento en que comienza su instalación.

Cómo protegerse

Comencemos por los móviles. Lo primero que debe hacer es asegurarse de que a su teléfono móvil solo accede usted. Muchos estudios de seguridad apuntan a que al menos el 25 por ciento de los usuarios de celulares no tienen activada siquiera una pantalla de bloqueo del terminal.

Actualmente los teléfonos inteligentes pueden ser bloqueados de numerosas maneras: contraseña, número PIN, patrones, a lo que se une, en los más modernos, la posibilidad de agregar datos biométricos, como la huella dactilar o el iris. Emplee entonces todos los métodos posibles para que nadie pueda desbloquear el celular sin su consentimiento. Eso sí, recuerde bien los patrones y contraseñas para que no termine devolviendo el terminal a sus opciones de fábrica con la consiguiente pérdida de datos.

Una vez que se haya asegurado del bloqueo del terminal, instale un software antivirus. Kaspersky y otros son lo suficientemente potentes para escanear el celular y encontrar si es afectado por *stalkerware*.

Si el móvil ha estado desprotegido y cree que pueda ser víctima de este tipo de software maligno, revise las aplicaciones instaladas y busque alguna que no conozca y pueda ser desinstalada.

Otras señales de un teléfono afectado por *stalkerware* es un rápido consumo de la batería, así como sobrecalentamiento.

Para los usuarios de ordenadores, revisar los programas instalados es vital. Cualquier software que no recuerde haber puesto debe quitarlo al momento.

Asimismo, es importante el uso de antivirus, y siempre es bueno bloquear el equipo cuando no se use, pero esté encendido.

En cuanto a las contraseñas, usa alguna única y difícil de predecir. Si la computadora la comparte con alguien más, trate de no digitalizar tantos detalles de su vida en ella.

http://www.juventudrebelde.cu/suplementos/informatica/2020-07-29/stalkerware-la-otra-pandemia-a-la-sombra-del-coronavirus