Fuente:
TyN Magazine

¿Qué es el Stalkerware?

Stalkerware es un software malicioso que permite a otra persona acceder a tu dispositivo o actividad sin tu consentimiento, y puede hacer cosas que van desde rastrear tu ubicación, acceder a tus fotos y archivos personales, interceptar correos y mensajes de aplicaciones como Whatsapp o Facebook, hasta escuchar llamadas y hacer grabar tus conversaciones sin que te des cuenta. En julio del año pasado, los Laboratorios contra Amenazas de Avast encontraron ocho aplicaciones de stalkerware para Android en la Play Store de Google, que indicaban haber sido descargadas más de 140,000 veces. A pesar de haber detectado esta amenaza y estar en constante monitoreo de nuevas iteraciones, los desarrolladores de este tipo de herramientas se han puesto cada vez más creativos a la hora de difundirlas para ocultar las formas en que violan la privacidad de las personas y las políticas de las tiendas digitales.

Aquí te dejamos unos tips para encontrar y remover *stalkerware* en tus dispositivos:

- No des clic en archivos o links inusuales.

Primero, lo primero: evitar caer. Si recibes mensajes sospechosos por redes sociales, correo o mensaje de texto, como aquellos que te piden pagos o te incitan a seguir un link, podrían ser una alerta de que estás siendo el blanco de alguien. No des clic en ningún vínculo ni descargues archivos adjuntos de mensajes que no sepas bien de dónde vienen, ya que pueden ser intentos de phishing para llevarte a una descarga de stalkerware. Ten cuidado porque el atacante también podría haber imitado el nombre o correo del remitente para hacerte pensar que el mensaje viene de alguien que conoces.

- Revisa la configuración de seguridad de tu teléfono.

Si notas que tu dispositivo se está comportando raro, es posible que la configuración haya cambiado sin tu permiso; esto podría ser una señal de que tu dispositivo ha sido expuesto a un ataque, especialmente si cambió después de haber estado perdido o si alguien más lo tomó. Uno de los mayores indicadores de stalkerware instalado es que estén activadas las descargas de fuentes externas a la App Store de Apple o la Play Store de Google, evidenciando que tu dispositivo ha sido intervenido para instalar el software. Asegúrate que las únicas vías de instalación de aplicaciones sean legítimas y, si tienes un Android, revisa que la opción de “Fuentes Externas” o “Aplicaciones desconocidas” esté desactivada en tus opciones de seguridad.

Si sospechas que el stalkerware ha sido instalado, echa un vistazo a todas las aplicaciones que tengas instaladas y elimina cualquiera que no reconozcas. También es importante actualizar tu sistema operativo a la última versión si no lo has hecho aún, ya que tienden a incluir actualizaciones de seguridad para tu dispositivo. Después de esto, deja que tu antivirus examine tu teléfono para buscar actividad sospechosa.

- Cambia tus contraseñas.

Si te preocupa que tu dispositivo haya sido vulnerado, cambia tu NIP y las contraseñas de tus cuentas más importantes, como correo y redes sociales, cuanto antes. Activar la autenticación de dos factores en tus cuentas añadirá una capa extra de protección. También renueva los métodos de desbloqueo, como huellas digitales, contraseñas o de reconocimiento facial. Si sigues sospechando que hay stalkerware instalado, hacer un reinicio de fábrica puede ser una opción para eliminar algunos tipos de software malicioso.

Disponible en:

https://www.tynmagazine.com/como-evitar-que-nos-vigilen-a-traves-del-cel... [1]

Links
[1] https://www.tynmagazine.com/como-evitar-que-nos-vigilen-a-traves-del-celular/