Publicado en Madrid el 04/04/2019

# Check Point indica las 4 señales que indican que un móvil ha sido hackeado

## Comprobar la 'salud' de un smartphone es mucho más sencillo de lo que parece y puede ahorrar muchos problemas

Se vive en la era de la tecnología donde el smartphone es sin lugar a duda el dispositivo más importante, aunque en muchas ocasiones el menos protegido. Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder especializado en ciberseguridad a nivel mundial, explica cómo saber si un dispositivo móvil está hackeado y poder así evitar males mayores.

"El teléfono móvil se ha convertido en un dispositivo fundamental en nuestro día a día, no sólo en el ámbito personal, sino también el profesional", señala Eusebio Nieva, director técnico de Check Point para España y Portugal. "Además, son un blanco fácil para los ciberdelincuentes, ya que suelen estar desprotegidos y permiten lanzar ataques tanto dirigidos como masivos. Por este motivo, el malware móvil es uno de los grandes problemas en materia de ciberseguridad a los que nos enfrentamos hoy en día", añade.

Entre las principales consecuencias derivadas de que un teléfono móvil haya sido hackeado se encuentra el hecho de que, una vez rastreado el dispositivo, se puedan realizar estafas de phishing contra el usuario, lo que permite a atacante llevar a cabo operaciones de recopilación de información increíblemente eficientes. Asimismo, los cibercriminales utilizan el dispositivo móvil como una de las principales armas de espionaje, ya que utilizan la cámara, GPS y micrófono del smartphone en cualquier momento y en cualquier lugar sin su consentimiento.

Señales que indican que un teléfono ha sido hackeado

Más allá del antivirus, para saber si la seguridad e integridad de un smartphone se ha visto comprometida, el usuario debe hacerse algunas preguntas que serán de gran utilidad a la hora de descubrir si hay alguien más haciendo uso de su teléfono móvil. Estas son las señales que indican que un teléfono ha sido hackeado:

Rendimiento: el desempeño del dispositivo es un claro indicador de su 'salud'. Si de repente su funcionamiento empieza a ser más lento de lo habitual, entonces puede ser que haya un malware que esté ralentizando el smartphone. Una prueba sencilla para comprobarlo es ver a qué velocidad se conecta a la red. Asimismo, la lentitud suele venir acompañada por un uso excesivo de la batería y un sobrecalentamiento, como consecuencia de que el malware se ejecuta de forma constante en segundo plano, lo que obliga al procesador a trabajar durante largos periodos de tiempo a su máxima velocidad.

Pop-ups: si cada vez que se desbloquea el teléfono el usuario recibe notificaciones con publicidad o anuncios, entonces hay un adware instalado en ese smartphone. Estas ventanas emergentes tienden a aparecer después de descargar e instalar alguna aplicación, que por lo general suelen ser de utilidades u optimizadores de memoria RAM. Estos pop-ups muestran mensajes muy variados, desde

invitaciones al store para descargar una determinada aplicación hasta alertar sobre la existencia de un virus móvil.

Mensajes desconocidos: la gran mayoría de malware para Android utiliza el número móvil para subscribirlo de forma unilateral a servicios premium, por lo que el usuario comenzará a recibir mensajes de servicios (horóscopo, etc.) que no conoce. Por otra parte, es posible que no sólo esté recibiendo estos mensajes, sino que también esté enviándolos a sus contactos sin que el propietario se dé cuenta, o incluso que algunos mensajes sean publicados en redes sociales. Además de los riesgos asociados al malware, el usuario corre el peligro de verse afectado en términos económicos.

Descarga de apps: el auge de las aplicaciones móviles hace que la tendencia sea a instalar un número mayor de estas en un dispositivo. Sin embargo, muchas veces el exceso de este tipo de utilidades hace que la gente no se de cuenta de que algunas se descargan sin permiso. Además, muchas veces estas aplicaciones no se pueden eliminar, por lo que el malware puede prolongar sus efectos en el dispositivo. Por otra parte, este hecho también implica un aumento significativo en el uso de datos, lo cuál puede servir como indicador de que algo no va bien en el smartphone.

"Aunque en líneas generales somos muy conscientes de lo importante que es proteger la información de nuestro teléfono móvil, lo cierto es que tomamos muy pocas medidas de protección para evitar que nuestro smartphone sea hackeado. Sin embargo, no hace falta ser experto en tecnología para comprobar que nuestro teléfono móvil está funcionando correctamente y con todas las garantías, ya que gracias a estas sencillas claves los usuarios pueden comprobar rápidamente si su dispositivo presenta algún tipo de problema y, por tanto, ponerle remedio de inmediato", explica Eusebio Nieva.

**Datos de contacto:**
Everythink PR

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional E-Commerce Software Ciberseguridad Dispositivos móviles