Últimamente se han popularizado un método de explotar las vulnerabilidades en los teléfonos y que actúan de manera efectiva utilizando medios seguros como formas de obtener datos de tu teléfono o hacer que tu teléfono trabaje para otros.

La primera explotación de vulnerabilidad es instalarte un juego o programa de forma segura, inclusive te la has podido bajar e instalar de la tienda oficial de Google Play. Advertir que aunque siempre se están mejorando y eliminando las aplicaciones y juegos desde Google, este tipo de aplicaciones pueden pasar inadvertidas por el programa oficial que analiza y bloquea las aplicaciones que pueden incluir malware o explotación de servicios del teléfono.

De esta forma te descargas la aplicación de forma normal, la aplicación funciona correctamente y parece que todo va bien, pero mientras, el teléfono funciona de forma exclavizada, siendo utilizado sin que tu te des cuenta como un dispositivo de minador de bitcoins, favoreciendo a otra persona (el publicador de la aplicación en la Tienda) que utiliza tu dispositivo ilegalmente sin tu permiso, para que tras su funcionamiernto enmascarado le busque criptomonedas, obteniendo grandes ganancias.

Este tipo de acciones se llama CriptoJacking y se producen tanto en dispositivos móviles como en ordenadores portátiles y de sobremesa. Trabajas gratis para otras personas sin saberlo.

¿Cómo saber si han realizado en un CriptoJacking en mi teléfono?

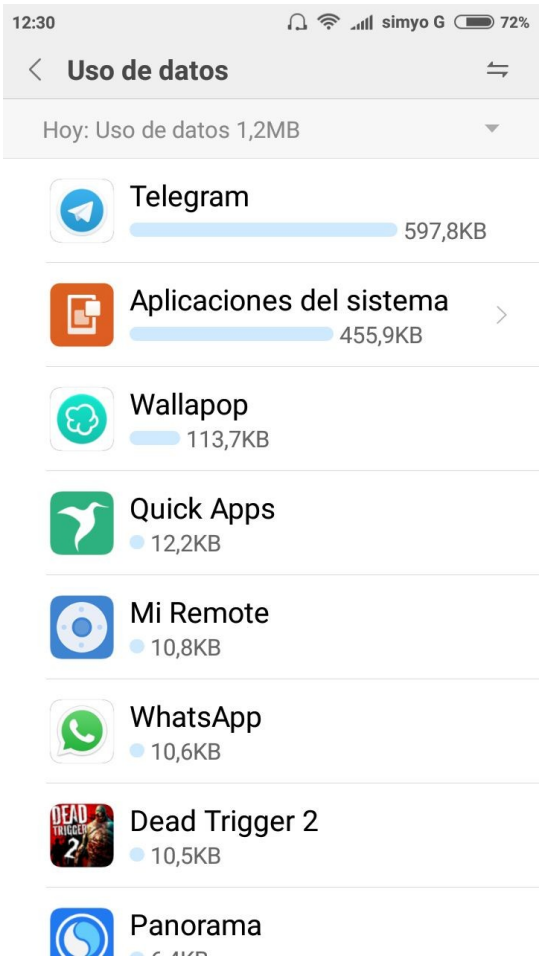
1.- Observa si al acceder a una aplicación o juego tarda más tiempo en ejecutarse o se ralentiza cuando estas utilizándola (esa aplicación no tiene porque ser la aplicación "infectada", sólo nos va a dar un indicativo de que hay algo más ejecutándose en el teléfono que no vemos, que está volviendo lento el teléfono) Aunque este no es indicativo 100% fiable pues hay apps infectadas que sólo funciona cuando no estamos utilizando el teléfono y en cuanto cogemos el teléfono para realizar una tarea, la app infectada se apaga)

2.- Observa si tienes que recargar más a menudo el teléfono: eso significa que alguna app (probablemente infectada) esta funcionando todo el tiempo (criptando monedas) para otros.

3.- Observa el consumo de datos y coloca avisos de uso de tarifa de datos en tu teléfono de forma que puedas darte cuenta de que alguna app está funcionando sin tu consentimiento (enviando y recibiendo datos) y si tienes tarifa limitada de datos puedes también evitar sorpresas desagradables al final de mes cuando te venga la factura telefónica o te agoten todos los datos disponibles para usar ese mes.

4.- Comprueba que aplicaciones instaladas últimamente han realizado un uso exagerado y abusivo de la batería. Hazlo durante varios días, hasta estar en lo cierto que esa es la aplicación que esta infectada.

5.- Comprueba también el estado de uso de la red y de igual forma tras varios días de observación comprueba la aplicación que ha estado la mayor parte del tiempo conectada en la red, ha consumido más datos o ha estado consumiendo datos aún sin haber estado usándola.



6.- Una vez localizado la app (aplicación o juego) que sobrepasa los límites de tu sospechas y estás seguro que es una aplicación o juego malicioso, simplemente con su desinstalación se suele acabar el problema, pero puede ser una aplicación maliciosa avanzada y sobre todo si tenías realizado un root en tu teléfono, puede que no se deje desinstalar o haga (de forma ilusoria) como que se ha desinstalado y realmente no lo haga, por lo que tendrás que realizar acciones más contundentes como restablecer tu teléfono a los valores de fábrica (formatearlo). Acuérdate de hacer un backup antes de todo, menos de los programas, que deberás decargarte nuevamente, evitando instalar de nuevo la aplicación maliciosa. Acuérdate también de reportar a Google esa app para que la retiren de la Tienda y evitar que el “hacker” siga ganando dinero de forma ilegal.