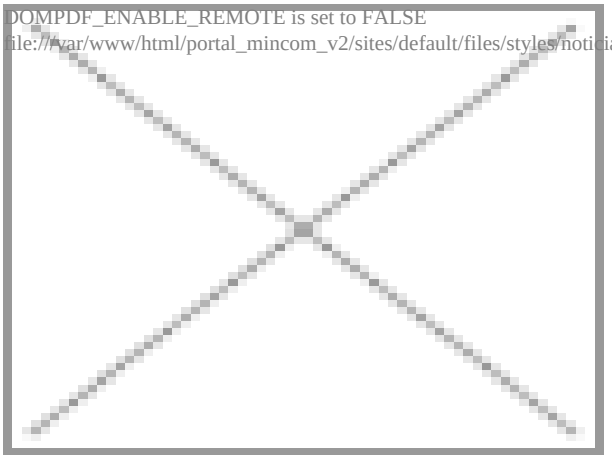

Fuente:
BBC

¿Existe algo peor para nuestro celular que un virus malicioso que intente acabar con todos los archivos en el dispositivo?

Parece que sí: un programa que intente lo mismo, pero que ningún antivirus pueda remover y reparar.

La empresa de seguridad informática Lookout informó esta semana sobre la aparición de un virus malicioso que se disfraza de populares aplicaciones como Facebook, Snapchat y Twitter y que es imposible de remover de los dispositivos móviles una vez se descarga en el sistema.

Y por si eso fuera poco, utiliza uno de los sistemas operativos más populares en el mundo para propagarse: Android.

Pero, ¿cómo actúa este malware?

"Hemos detectado al menos 20.000 muestras de este virus tipo troyano enmascarado bajo legítimas aplicaciones como *Facebook*, *Candy Crush*, *NYTimes* y *WhatsApp*", le dijo a BBC Mundo Michael Bentley, Jefe de Investigación de Lookout.

"Lo que hace el pirata informático es tomar la aplicación de Google Play –la tienda de Android de donde se bajan las apps-, 'reempaquetarla' con el virus malicioso y después ubicarla en otras tiendas virtuales de venta de aplicaciones", agregó.

Entonces los usuarios bajan, por ejemplo Facebook, con la confianza de que es un proceso seguro –de hecho, la aplicación reempaquetada funciona adecuadamente-, pero de manera automática y casi sin que el usuario se entere instala un virus en lo que se conoce como la "corazón" del teléfono móvil: el directorio raíz.

Y de allí no vuelve a salir.

"Cuando el teléfono está infectado con este nuevo y sofisticado programa malicioso es imposible removerlo y la única opción es cambiar de teléfono", anotó Bentley.

Más sofisticado

En el pasado se había visto como los "adware" o programas dedicados a instalar publicidad de forma

invasiva en los celulares se habían convertido en una amenaza para sus usuarios.

Sin embargo, como lo explica Bentley, la mayoría de esos adware se podían remover del sistema sin tener que deshacerse del teléfono o enviarlo a costosos expertos en informática para su reparación.

Este virus es un paso hacia adelante en este tipo de "invasiones".

Y todo con un solo objetivo: ganar más dinero.

Al no poder desinstalarlo del sistema, este nuevo tipo de virus malicioso continúa mostrando anuncios sin parar, hasta que al usuario solo le queda una opción: deshacerse del teléfono.

"Hemos visto que los virus troyanos que buscan ganar dinero mediante el adware invasivo están tomando tres caminos hacia su sofisticación: mejores y más seguras formas de ganar dinero, mayor acceso a la información del usuario e incremento del riesgo", explicó Bentley.

Los métodos para ganar dinero, de acuerdo a Lookout, están enfocados en buscar la forma en que, una vez instalado este virus malicioso, el pirata informático acceda al "corazón" del sistema y pueda continuar enviando los mensajes publicitarios que desee.

Además de adueñarse de la información básica que consignamos en nuestros dispositivos y que después puede ser vendida en base de datos a terceros.

"Pero lo más preocupante es el incremento del riesgo, porque pusieron en evidencia de una forma muy clara la intención del malware: camuflarse y pasar desapercibido en el sistema", explicó Bentley.

"Lo que es un claro signo de que en el futuro llegarán nuevos virus que no van a poder ser rastreados y van a poder obtener toda la información que deseen sin que el usuario se entere", agregó.

¿Cómo identificarlo?

Aunque el virus utiliza la fachada de estas reconocidas aplicaciones existe una forma de evitar que este virus "irrevocable" se instale en el directorio raíz.

"Las aplicaciones que se bajan o compran en Google Play están libres de este virus malicioso. Si tienes un teléfono con Android, hay que evitar bajar Twitter o Snapchat de otros lugares que no sean de su tienda oficial", señaló.

¿Y una posible solución distinta a deshacerse del teléfono? Pocas.

"Hay una opción que es reinstalar un nuevo directorio raíz, que debe ser hecho por personas especializadas que por lo general cobran más de lo que vale un teléfono en el mercado", anotó Bentley.

Y agregó: "La principal recomendación es bajar las aplicaciones de las tiendas oficiales y tener un buen antivirus para evitar que malware como este se instale y ya sea imposible sacarlo del sistema".

Disponible en: http://www.bbc.com/mundo/noticias/2015/11/151106_tecnologia_virus_adware... [1]

Links
[1]

http://www.bbc.com/mundo/noticias/2015/11/151106_tecnologia_virus_adware_sin_solucion_lookout_amv