Masterhacks – Kaspersky descubrió un malware, específicamente spyware, que es capaz de burlar las defensas de la empresa Apple, que afirma innecesarios los antivirus para sus iPhone. De igual forma, afecta al sistema Android.

Se trata de Pegasus, un spyware que recopila información almacenada en el dispositivo y que es capaz de monitorizar de forma constante la actividad que se realiza en el dispositivo.

La compañía de seguridad afirma que se trata de una total vigilancia, debido a que Pegasus es un malware modular que instala las partes necesarias para leer mensajes del usuario y correo, escuchar llamadas, realizar capturas de pantalla, registrar pulsaciones de teclas, acceder al historial del navegador, a los contactos, entre otras acciones.

Este malware también podría escuchar audios codificados y leer mensajes cifrados, debido a su keylogging y sus capacidades de grabación de audio.

Además, es capaz de autodestruirse, ya que si no puede comunicarse con el servidor de control remoto luego de 60 días, se desinstala solo, de igual forma lo hace si detecta que se ha insertado en el dispositivo equivocado con la tarjeta SIM incorrecta.

Existe una versión para Android conocida como Chrysaor, que es muy similar a la versión para iOS en términos de capacidades, pero es diferentes en cuando a las técnicas de penetración.

Pegasus para Android no se basa en las vulnerabilidades de día cero. Utiliza un método de enraizamiento llamado Framaroot.

En la versión para iOS, si el virus no realiza su propio jailbreak al dispositivo, el ataque fallará, en cambio en Android, si el software malicioso no obtiene acceso al root para instalarse, se disfraza de una app que requiere permisos como cualquier otra para ingresar al dispositivo, con la finalidad de que el usuario los acepte sin saber que se trata de un virus.

Kaspersky proporciona tres consejos para evitar la instalación de software malicioso:

1.- Actualizar los dispositivos siempre y prestar atención a las actualizaciones de seguridad.

2.- Instalar una app de seguridad en cada dispositivo, no existe ninguna para iOS, pero se espera que con la aparición de Pegasus, Apple reconsidere su postura.

3.- Evitar caer en suplantación de identidad. Si se recibe un vínculo de fuente desconocida, no hacer clic en este.