Ya apareció malware que se aprovecha del Pokemon GO

17/07/2016

Esta versión para dispositivos Android ha sido alterada con una herramienta de acceso remoto (RAT por sus siglas en inglés) llamada Droidjack que podría permitir el control del teléfono móvil por parte de los ciberdelincuentes.

Por el momento, el juego de realidad aumentada solo está disponible de manera oficial en Estados Unidos, Australia, Reino Unido y Nueva Zelanda; sin embargo, su popularidad ha escalado rápidamente alrededor del mundo, lo que ha incitado a los usuarios de Android en otros países, incluyendo algunos de América Latina, a descargar versiones de la app a través de canales ilegítimos.

Para estas versiones, los usuarios de Android requieren ajustar la configuración de su dispositivo de manera que les permita instalar archivos con extensión APK, provenientes de fuentes no confiables, una práctica considerada de alto riesgo.

Si bien, a la fecha aún no se ha detectado en circulación el archivo APK que contiene el RAT, éste ya fue descubierto en un repositorio de archivos maliciosos, por lo que podría propagarse en línea en cualquier momento.

"El uso de juegos en línea populares como vector para la instalación de malware es una práctica común, por lo que es sólo cuestión de tiempo para que los ciberdelincuentes aprovechen la popularidad de Pokémon GO para infectar a consumidores impacientes y confiados. La mejor manera de proteger su dispositivo e información es

instalando sólo aplicaciones descargadas a través de tiendas oficiales y complementar esto con una solución de seguridad robusta", comentó Roberto Martínez, experto en seguridad de Kaspersky Lab.

El archivo APK malicioso solicita visibilidad sobre las conexiones de Wi-Fi con la finalidad de conectarse o desconectarse de la red, cambiar la conectividad y recabar datos de aplicaciones que estén corriendo. Además, la versión alterada de Pokémon GO se comunica con un dominio de comando y control albergado en una dirección IP dinámica en Turquía. El espacio de las IP dinámicas comúnmente es utilizado para alojar redes de bots, envío de spam, así como otras actividades sospechosas. En este caso, el dominio se encuentra alojado en No-IP.org, un sitio que los cibercriminales han utilizado en el pasado para ocultar operaciones de malware.

Para evitar que su dispositivo sea comprometido por este malware, Kaspersky Lab les ofrece a los usuarios las siguientes recomendaciones:

-No tome atajos y esperen que la versión oficial de este juego esté disponible en su país

- No desactive la solución antimalware de su dispositivo para facilitar la instalación de software ya que no solo expondrá a su Smartphone a ser vulnerado, pero también a la información que este almacena.

-No descargue la aplicación desde una fuente no verificada. Hacerlo lleva un riesgo demasiado alto que no vale la pena correr."