Loapi es un nuevo troyano que ha afectado a miles de usuarios de distintos países, entre ellos México. Este malware para Android tiene una arquitectura modular compleja que le permite realizar varias acciones en los dispositivos infectados.

Kaspersky Lab informa que dada su arquitectura, Loapi es capaz de realizar funciones casi ilimitadas en un dispositivo. Sus alcances van desde minería de criptomonedas hasta ataques DDoS.

Dmitry Bestuzhev, director del Equipo de Investigación y Análisis de Kaspersky para América Latina, menciona que lo que le llama la atención es que además de estar en la lista de los países más afectados, México también ocupa el cuarto lugar a nivel de ataques registrados por la familia de malware móvil, seguido por Brasil, Chile, Panamá y Perú.

Loapi se propaga por medio de campañas publicitarias que parecen ser soluciones de antivirus o aplicaciones para adultos.

Cuando se instalan, las apps solicitan derechos de administrador del dispositivo y de forma discreta comienzan comunicación con los servidores de mando y control para la instalación de módulos adicionales.

Cuando el dispositivo se infecta, eliminar la app es muy difícil, ya que Loapi puede protegerse.

> *«Tan rápido como se intente revocar los derechos de administrador del dispositivo, el malware bloqueará la pantalla del dispositivo y cerrará la ventana. También puede recibir una lista de aplicaciones que representan un peligro para él desde los servidores de mando y control»,* afirman los investigadores de Kaspersky.

Aparte de esto, el malware genera una carga de trabajo demasiado pesada, lo que ocasionaría que el dispositivo se sobrecaliente y deforme la batería, lo que causaría otros daños físicos.

> *«El riesgo inesperado que conlleva este malware es que, aún cuando no se causen daños financieros directos al usuario al robar los datos de sus tarjetas, sí puede destruir el teléfono. Esto no es algo que la gente esperaría de un troyano de Android, ni siquiera de los más avanzados».*