Zoopark es un malware para Android que accede a los datos de aplicaciones como WhatsApp y Telegram. Es capaz de tener acceso a contraseñas, fotos, videos, realizar capturas de pantalla y robar las conversaciones del usuario.

Este virus comenzó robando datos de contactos almacenados, pero ha estado evolucionando y se ha convertido en un malware complejo que supera a muchos de los que existen para este sistema operativo.

Kaspersky Lab, compañía de seguridad, informó que se desconoce el origen del malware, pero se cree que fue creado por algún gobierno.

Según la compañía de seguridad informática, el virus puede acceder a contactos, información de cuentas del usuario, historial de llamadas, mensajes de texto, favoritos e historial del navegador, grabar llamadas, enviar datos del portapapeles, historial de búsqueda del navegador y ubicación del dispositivo.

Además, puede obtener información general del dispositivo, información de las aplicaciones instaladas, archivos en la tarjeta de memoria, documentos almacenados en el dispositivo, información que se introduce en el teclado y datos almacenados en aplicaciones, también es capaz de tomar una foto con la cámara frontal y enviarla.

La forma de infección es cuando se descarga involuntariamente al acceder a algunos sitios web no seguros. Según Kaspersky, el principal objetivo del spyware es espiar a personas de Oriente Medio. La compañía asegura que el usuario común no debe temer al malware, ya que solo se utiliza para ataques dirigidos y no de forma aleatoria.

«Está programado para infectar una audiencia específica», explicó en su sitio web.

Aún así, es necesario tomar acciones precautorias para evitar infectarse con este tipo de malware, como descargar aplicaciones de fuentes confiables, actualizar el sistema operativo y apps y la instalación de algún antivirus si navegas mucho por Internet.