Investigadores de seguridad cibernética descubrieron un nuevo troyano que roba información, dirigido a los dispositivos Android, que cuenta con una gran cantidad de capacidades de exfiltración de datos, desde la recopilación de búsquedas en el navegador hasta la grabación de audio y llamadas telefónicas.

Aunque el malware en Android antes se ha disfrazado de aplicaciones similares, que tienen nombres parecidos a piezas de software legítimas, esta nueva y sofisticada aplicación maliciosa se hace pasar por una aplicación de actualización del sistema para tomar el control de los dispositivos comprometidos.

> *«El software espía crea una notificación si la pantalla del dispositivo está apagada cuando recibe un comando mediante el servicio de mensajería Firebase. 'Buscando actualización...' no es una notificación legítima del sistema operativo, sino del software espía»*, dijeron los investigadores de Zimperium.

Al instalarse la aplicación, la sofisticada campaña de software espía comienza al registrar el dispositivo con un servidor de comando y control (C2) de Firebase, con información como el porcentaje de batería, estadísticas de almacenamiento y si el teléfono tiene WhatsApp instalado, seguido de la acumulación y exportación de cualquier dato de interés para el servidor en forma de archivo ZIP cifrado.

El spyware presenta innumerables capacidades con un enfoque sigiloso, incluidas tácticas para robar contactos, marcadores del navegador e historial de búsqueda, robar mensajes al abusar de los servicios de accesibilidad, grabar audio y llamadas telefónicas y tomar fotos con las cámaras del teléfono. También puede rastrear la ubicación de la víctima, buscar archivos con extensiones específicas y obtener datos del portapapeles del dispositivo.

> *«La funcionalidad del software espía y la exfiltración de datos se activan bajo múltiples condiciones, como un nuevo contacto agregado, un nuevo SMS recibido o una nueva aplicación instalada haciendo uso de los receptores contentObserver y Broadcast de Android»*, dijeron los investigadores.

Además, el malware no solo organiza los datos recopilados en distintas carpetas de su almacenamiento privado, sino que también elimina cualquier rastro de actividad maliciosa al eliminar los archivos ZIP tan pronto como recibe un mensaje de 'éxito' del servidor C2 después de la exfiltración. En un intento adicional por evadir la detección y pasar desapercibido, el software espía también reduce su consumo de ancho de banda al cargar miniaturas en lugar de las imágenes y videos reales presentes en el almacenamiento externo.

Aunque la aplicación *«System Update»* nunca se distribuyó por medio de la tienda oficial de Google Play, la investigación destaca una vez más cómo las tiendas de aplicaciones de terceros pueden albergar malware peligroso. La identidad de los autores de malware, las víctimas objetivo y el motivo último de la campaña aún no están claros.