Se han descubierto dos aplicaciones de gestión de archivos en la tienda de Google Play que actúan como spyware, poniendo en peligro la privacidad y seguridad de hasta 1.5 millones de usuarios de Android. Estas aplicaciones llevan a cabo prácticas engañosas y envían de manera secreta datos sensibles de los usuarios a servidores maliciosos en China.

Pradeo, una destacada compañía de seguridad móvil, ha descubierto esta preocupante infiltración. El informe muestra que ambas aplicaciones de spyware, llamadas Recuperador de Archivos y Recuperador de Datos (com.spot.music.filedate) con más de 1 millón de instalaciones, y Administrador de Archivos (com.file.box.master.gkd) con más de 500,000 instalaciones, son desarrolladas por el mismo grupo. Estas aparentemente inofensivas aplicaciones para Android utilizan tácticas maliciosas similares y se ejecutan automáticamente al reiniciar el dispositivo sin necesidad de intervención del usuario.

A pesar de lo que afirman en la tienda de Google Play, donde ambas aplicaciones aseguran a los usuarios que no se recopila ningún dato, el motor de análisis de Pradeo ha descubierto que se recopilan varios datos personales sin el conocimiento de los usuarios. Los datos robados incluyen listas de contactos, archivos multimedia (imágenes, archivos de audio y videos), ubicación en tiempo real, código de país móvil, detalles del proveedor de red, código de red del proveedor de la tarjeta SIM, versión del sistema operativo, marca y modelo del dispositivo.

Lo que es particularmente alarmante es la gran cantidad de datos transferidos por estas aplicaciones de spyware. Cada aplicación realiza más de cien transmisiones, una cantidad considerable para actividades maliciosas. Una vez recopilados los datos, se envían a múltiples servidores en China, los cuales son considerados maliciosos por expertos en seguridad.

Para empeorar la situación, los desarrolladores de estas aplicaciones de spyware han utilizado tácticas sigilosas para aparentar mayor legitimidad y dificultar su desinstalación.

Los hackers han incrementado artificialmente el número de descargas de las aplicaciones mediante granjas de instalación o emuladores de dispositivos móviles, creando una falsa sensación de confianza. Además, ambas aplicaciones cuentan con permisos avanzados que les permiten ocultar sus iconos en la pantalla principal, lo que dificulta que los usuarios desprevenidos las desinstalen.

> *«Estas aplicaciones han sido eliminadas de Google Play. Google Play Protect protege a los usuarios de aplicaciones conocidas por contener este malware en dispositivos Android con los servicios de Google Play, incluso cuando dichas aplicaciones provienen de otras fuentes fuera de Play»*, declaró un portavoz de Google a The Hacker News.

Pradeo ofrece recomendaciones de seguridad para individuos y empresas a raíz de este inquietante descubrimiento. Los individuos deben ser cautelosos al descargar aplicaciones, especialmente aquellas sin calificaciones, si afirman tener una amplia base de usuarios. Es sumamente crítico leer y comprender los permisos de la aplicación antes de aceptarlos para prevenir brechas como esta.

Las organizaciones deben priorizar la educación de sus empleados acerca de las amenazas móviles y establecer sistemas automatizados de detección y respuesta móvil para protegerse de posibles ataques.

Este incidente resalta la continua batalla entre expertos en ciberseguridad y actores malintencionados que aprovechan a usuarios desprevenidos. Los ataques de malware y spyware evolucionan constantemente y encuentran nuevas formas de infiltrarse en plataformas confiables como la tienda de Google Play. Como usuario, es imperativo mantenerse alerta, ejercer cautela al descargar aplicaciones y confiar en fuentes confiables para obtener software.