Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°161	Fecha: 09-07-2023
		Página: 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Dos aplicaciones de spyware en Google Play con 1.5 millones de usuarios que envían datos a China		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

La empresa líder en seguridad móvil, Pradeo descubre dos aplicaciones de administración de archivos en Google Play Store son spyware, estas aplicaciones mediante técnicas engañosas envían de forma secreta los datos confidenciales de los usuarios hacia servidores maliciosos en China.

2. DETALLES:

Pradeo, una empresa líder en seguridad móvil, descubrió la infiltración de dos spyware ocultos en Google Play Store, estos llevan afectando hasta 1.5 millones de usuarios. Ambas aplicaciones de spyware: File Recovery y Data Recovery (com.spot.music.filedate) con más de 1 millón de instalaciones, y File Manager (com.file.box.master.gkd) con más de 500,000 instalaciones, son desarrolladas por el mismo grupo y se inician automáticamente cuando el dispositivo se reinicia sin la intervención del usuario.

En contrario, a lo afirmado por Google Play Store, el motor de análisis de Pradeo descubrió que los dos spyware recopilan datos de los usuarios sin su consentimiento. Entre los datos robados contienen 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 SIM, versión del sistema operativo, marca del dispositivo y modelo.

Lo más alarmante es la gran cantidad de datos transferidos por estas aplicaciones de spyware. Cada una realiza más de cien transmisiones, lo cual es significativo para actividades maliciosas. Una vez que se recopilan los datos, son enviados a múltiples servidores en China considerados maliciosos por los expertos en seguridad.

Además, los desarrolladores de estas aplicaciones utilizaron técnicas furtivas para aparentar ser más legítimos y dificultar su desinstalación. Incrementaron artificialmente el número de descargas con granjas de instalaciones o emuladores de dispositivos móviles, creando una falsa sensación de confiabilidad. Ambas aplicaciones también tienen permisos avanzados que les permiten ocultar sus iconos en la pantalla de inicio, lo que dificulta la desinstalación por parte de usuarios desprevenidos.

Pradeo ofrece recomendaciones de seguridad tanto para individuos como para empresas en respuesta a este descubrimiento alarmante. Se recomienda tener cuidado al descargar aplicaciones, especialmente aquellas sin calificaciones, aunque afirmen tener una gran base de usuarios. Es importante leer y comprender los permisos de las aplicaciones antes de aceptarlos para evitar vulnerabilidades como esta.

3. RECOMENDACIONES:

- Evitar descargar aplicaciones que no tengan reseñas mientras miles de usuarios.
- Leer las reseñas cuando las haya, generalmente reflejan la verdadera naturaleza de las aplicaciones.
- Leer cuidadosamente los permisos antes de aceptarlos.
- Sensibilizar a los colaboradores sobre amenazas móviles.
- Automatizar la detección y respuesta móvil para ofrecer una flexibilidad segura a los usuarios, examinando las aplicaciones y evitando su lanzamiento cuando no cumplan con su política de seguridad.

Fuente de Información:	• https://thehackernews.com/2023/07/two-spyware-apps-on-google-play-with-15.html • https://blog.pradeo.com/spyware-tied-china-found-google-play-store