

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°153			Fecha: 29-06-2023
				Página: 4 de 5
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL			
Nombre de la alerta	La aplicación espía de Android LetMeSpy sufre una importante violación de datos, exponiendo los datos personales de los usuarios			
Tipo de Ataque	Spyware	Abreviatura	Spyware	
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet			
Código de familia	C	Código de Sub familia	C04	
Clasificación temática familia	Código Malicioso			
Descripción				
<p>1. ANTECEDENTES:</p> <p>LetMeSpy (LMS) es una aplicación móvil gratuita para teléfono móvil con Android, realiza seguimiento de las ubicaciones de llamadas, SMS y GPS del teléfono en el que está instalado. Este programa es muy ligero y puede ser invisible para el usuario.</p> <p>El 21 de junio de 2023, LetMeSpy anunció en su web oficial ser víctima de una violación de seguridad, esta vulnerabilidad en su aplicación de monitoreo de teléfono basada en Android permitió que un ciberdelincuente robara datos confidenciales de los miles de usuarios de Android.</p> <p>A partir de enero 2023, la aplicación de Stalkerware (también conocido como spouseware o virus), es un tipo de spyware, principalmente orientado a dispositivos móviles inteligentes, cuyo objetivo es obtener y mandar los datos de sus víctimas a un servidor controlado por ciberdelincuentes. A la fecha se tiene conocimiento que fue empleado en rastrear 236 322 teléfonos en todo el mundo.</p> <p>También existen registros que indican que 13 000 dispositivos fueron comprometidos, de los cuales la mayoría de las víctimas se encuentran en EEUU, India y algunos países de África.</p> <p>2. DETALLES:</p> <p>La aplicación de monitoreo de teléfonos basada en Android, LetMeSpy, ha sufrido una violación de seguridad que resultó en el robo de datos confidenciales de miles de usuarios de Android. Los atacantes obtuvieron acceso a direcciones de correo electrónico, números de teléfono y contenido de mensajes recopilados en las cuentas de los usuarios. LetMeSpy informó del incidente a las autoridades policiales y de protección de datos, ha suspendido todas las funciones relacionadas con las cuentas afectadas. La identidad y los motivos del actor de la amenaza aún no se conocen.</p> <p>LetMeSpy es una aplicación de suscripción mensual que permite a los usuarios espiar a otros mediante la instalación del software en sus dispositivos. Ofrece una amplia gama de características de monitoreo, como registros de llamadas, mensajes SMS y geolocalizaciones. La aplicación se ha utilizado para rastrear más de 236,000 teléfonos en todo el mundo, recopilando millones de mensajes de texto, registros de llamadas y ubicaciones.</p> <p>La violación de seguridad revelada contiene alrededor de 26,000 direcciones de correo electrónico, 16,000 mensajes SMS y una base de datos de ubicaciones de víctimas. Los datos se remontan a 2013, cuando LetMeSpy comenzó a operar, y se han comprometido al menos 13,000 dispositivos. La mayoría de las víctimas se encuentran en Estados Unidos, India y partes de África.</p> <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Proteja su teléfono con una contraseña segura que nunca comparta con otra persona. • Solo descargue aplicaciones de fuentes oficiales, como Google Play o Apple App Store. • Cambie las contraseñas de todas sus cuentas periódicamente y no las comparta con nadie. • Instale una solución de seguridad informática fiable como, por ejemplo: Kaspersky for Android en los dispositivos y analícelos regularmente. En el caso de stalkerware ya instalado, este solo debe hacerse después de que se haya evaluado el riesgo para la víctima. 				
Fuente de Información:	<ul style="list-style-type: none"> • https://www.letmespy.com/es/ • https://thehackernews.com/2023/06/android-spy-app-letmespy-suffers-major.html • https://techcrunch.com/2023/06/27/letmespy-hacked-spyware-thousands/ • https://stopstalkerware.org/ 			