Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°213**	**Fecha: 10-09-2023**
		Página: 4 de 9

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Las aplicaciones de Android 'Evil Telegram' en Google Play infectaron 60.000 personas con software espía		
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

1. **ANTECEDENTES:**

Se instalaron más de 60.000 veces varios clones maliciosos de Telegram para Android en Google Play, infectando a las personas con software espía que roba mensajes de usuarios, listas de contactos y otros datos.

Las aplicaciones parecen estar diseñadas para usuarios de habla china y la minoría étnica uigur, lo que sugiere posibles vínculos con los bien documentados mecanismos estatales de vigilancia y represión.

Las aplicaciones fueron descubiertas por Kaspersky, quien las informó a Google. Sin embargo, en el momento en que los investigadores publicaron su informe, todavía había varias aplicaciones maliciosas disponibles para descargar a través de Google Play. Las aplicaciones de Telegram presentadas en el informe de Kaspersky se promocionan como alternativas "más rápidas" a la aplicación normal.

Los ejemplos que se muestran en el informe tienen más de 60 000 instalaciones, por lo que la campaña tiene un éxito moderado a la hora de llegar a un grupo de objetivos potenciales.

2. **DETALLES:**

Los analistas de seguridad informan que las aplicaciones son aparentemente las mismas que el Telegram original, pero contienen funciones adicionales en el código para robar datos.

Según el investigador de seguridad de Kaspersky, Igor Golovin, las aplicaciones vienen con funciones nefastas para capturar y exfiltrar nombres, identificaciones de usuarios, contactos, números de teléfono y mensajes de chat a un servidor controlado por actores. La actividad ha recibido el nombre en código Evil Telegram de la empresa rusa de ciberseguridad.

Cuando el usuario recibe un mensaje a través de la aplicación troyanizada, el software espía envía una copia directamente al servidor de comando y control (C2) del operador en "sg[.]telegrnm[.]org".

Los datos exfiltrados, que se cifran antes de la transmisión, contienen el contenido del mensaje, el título y la identificación del chat/canal, y el nombre y la identificación del remitente.

La aplicación de software espía también monitorea la aplicación infectada en busca de cambios en el nombre de usuario e identificación de la víctima y cambios en la lista de contactos y, si algo cambia, recopila la información más actualizada.

Cabe señalar que las aplicaciones maliciosas de Evil Telegram utilizaron los nombres de paquete 'org.telegram.messenger.wab' y 'org.telegram.messenger.wob', mientras que la aplicación legítima de Telegram tiene un nombre de paquete de 'org.telegram.messenger .web.'

Desde entonces, Google eliminó estas aplicaciones de Android de Google Play.

3. **RECOMENDACIONES:**

- Utilizar sólo versiones originales de aplicaciones de mensajería.
- Evitar descargar aplicaciones bifurcadas que prometen mayor privacidad, velocidad u otras funciones.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/evil-telegram-android-apps-on-google-play-infected-60k-with-spyware/ • hxxps://thehackernews.com/2023/09/millions-infected-by-spyware-hidden-in.html