Los expertos en ciberseguridad han identificado aplicaciones maliciosas para Android que utilizan las marcas de Signal y Telegram y que se distribuyen a través de la Google Play Store y la Samsung Galaxy Store. Estas aplicaciones están diseñadas para introducir el spyware BadBazaar en dispositivos infectados.

La compañía eslovaca ESET ha atribuido esta campaña a un grupo relacionado con China denominado GREF.

> *«Es muy probable que estas campañas estén en marcha desde julio de 2020 y julio de 2022, respectivamente. Han utilizado la tienda Google Play, la Samsung Galaxy Store y sitios web específicos para distribuir el código de espionaje BadBazaar en versiones falsas de las aplicaciones Signal Plus Messenger y FlyGram»,* informó Lukáš Štefanko, un investigador de seguridad, en un nuevo informe.

Las víctimas en su mayoría han sido identificadas en Alemania, Polonia y Estados Unidos, seguidas de Ucrania, Australia, Brasil, Dinamarca, Congo-Kinshasa, Hong Kong, Hungría, Lituania, los Países Bajos, Portugal, Singapur, España y Yemen.

BadBazaar fue descubierto por primera vez por Lookout en noviembre de 2022 y estaba dirigido a la comunidad uigur en China. Este spyware se escondía detrás de aplicaciones aparentemente inofensivas para Android e iOS que, una vez instaladas, recopilaban una amplia variedad de datos, incluyendo registros de llamadas, mensajes SMS, ubicaciones y más.

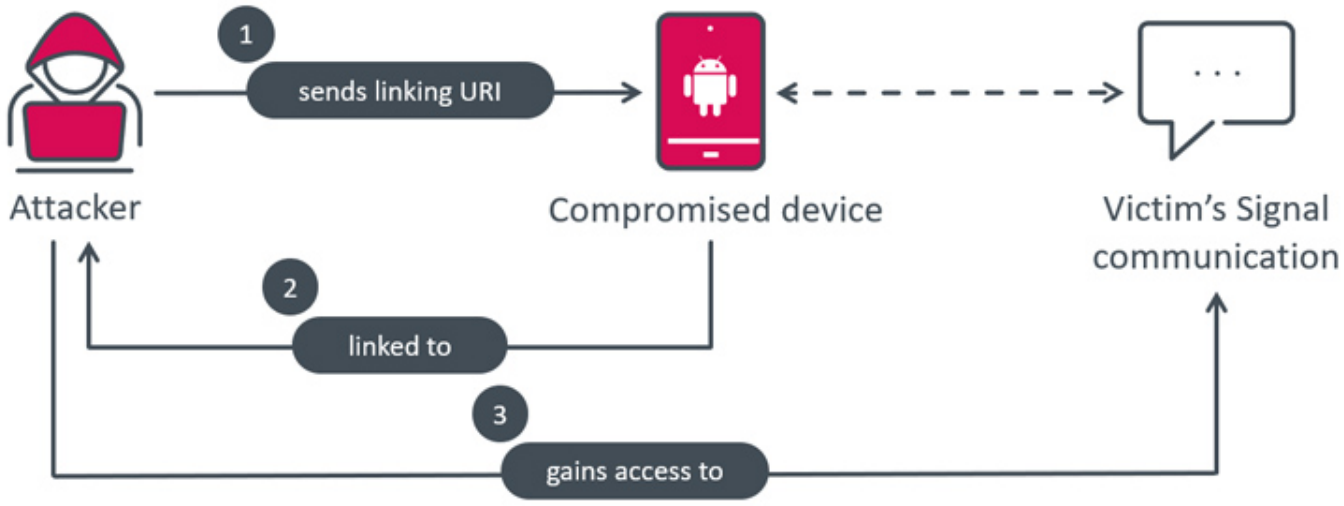
La campaña anterior, que estaba activa desde al menos 2018, es también notable por el hecho de que las aplicaciones maliciosas para Android nunca se publicaron en la Play Store. Aunque ambas aplicaciones han sido retiradas de la tienda de aplicaciones de Google, siguen disponibles en la Samsung Galaxy Store.

Los detalles de las aplicaciones son los siguientes:

- Signal Plus Messenger (org.thoughtcrime.securesmsplus): Ha tenido más de 100 descargas desde julio de 2022 y también se puede obtener en signalplus[.]org.
- FlyGram (org.telegram.FlyGram): Ha tenido más de 5,000 descargas desde junio de 2020 y también se puede obtener en flygram[.]org.

Además de estos métodos de distribución, se cree que posibles víctimas también han sido engañadas para instalar estas aplicaciones a través de un grupo de Telegram uigur que se dedica a compartir aplicaciones de Android. Este grupo cuenta con más de 1,300 miembros.

Tanto Signal Plus Messenger como FlyGram están diseñadas para recolectar y enviar datos sensibles de usuarios, y cada una de estas aplicaciones está dedicada a recopilar información de las aplicaciones que intentan imitar: Signal y Telegram.



Esto implica la capacidad de obtener acceso al PIN de Signal y a las copias de seguridad de las conversaciones de Telegram en caso de que la víctima habilite la función de Sincronización en la nube desde la aplicación modificada.

En una interesante novedad, Signal Plus Messenger representa el primer caso documentado de vigilancia de las comunicaciones de Signal al conectar de manera oculta el dispositivo

comprometido a la cuenta de Signal del atacante sin necesidad de ninguna interacción por parte del usuario.

> *«BadBazaar, el malware responsable de esta vigilancia, evita el procedimiento convencional de escanear el código QR y hacer clic por parte del usuario, al recibir la URI necesaria directamente desde su servidor de control y ejecutar automáticamente la acción requerida cuando se presiona el botón 'Enlazar dispositivo'»*, explicó Štefanko.

> *«Esto permite que el malware enlace de forma encubierta el teléfono del usuario al dispositivo del atacante, lo que les permite espiar las comunicaciones de Signal sin que la víctima lo advierta».*

Por otro lado, FlyGram también incorpora una característica denominada «*anclaje SSL*« para eludir el análisis al incrustar el certificado en el archivo APK, de modo que solo permite comunicación cifrada con el certificado previamente definido, lo que complica la interceptación y el análisis del tráfico de red entre la aplicación y su servidor.

Un análisis de la función de Sincronización en la nube de la aplicación también revela que cada usuario que se registra en el servicio recibe una ID única que se incrementa secuencialmente. Se estima que 13,953 usuarios (incluyendo a ESET) instalaron FlyGram y activaron la función de Sincronización en la nube.

A pesar de informes previos de código abierto que relacionaban al grupo GREF con APT15, debido a la falta de pruebas definitivas, ESET continúa rastreando a GREF como un grupo independiente.

> *«El propósito principal de BadBazaar es recopilar información del dispositivo, la lista*

> *de contactos, los registros de llamadas y la lista de aplicaciones instaladas, además de realizar espionaje en los mensajes de Signal al conectar en secreto la aplicación Signal Plus Messenger del usuario al dispositivo del atacante»*, concluyó Štefanko.