Aplicaciones troyanizadas de Telegram y Signal distribuyen el código espía entre usuarios de Android

El equipo de investigación de ESET, compañía líder en detección proactiva de amenazas, identificó dos campañas activas dirigidas a usuarios de Android, donde los actores de amenazas detrás de la herramienta se atribuyen al grupo APT (Advanced Persistent Threat) GREF, alineado con China. Probablemente activas desde julio de 2020 y julio de 2022, las campañas distribuyeron el código de espionaje de Android BadBazaar a través de Google Play Store, Samsung Galaxy Store y sitios web dedicados que representan las aplicaciones maliciosas Signal Plus Messenger y FlyGram.

Los actores de la amenaza parchearon las apps de código abierto Signal y Telegram para Android con el código malicioso identificado como BadBazaar.
Basándose en su telemetría, ESET identificó campañas activas de Android en las que un atacante subió y distribuyó aplicaciones maliciosas que responden a los nombres de Signal Plus Messenger y FlyGram a través de Google Play Store, Samsung Galaxy Store y sitios web dedicados, imitando la aplicación Signal (signalplus[.]org) y una aplicación alternativa de Telegram (flygram[.]org).

El objetivo de estas aplicaciones troyanizadas es filtrar datos de los usuarios. En concreto, FlyGram puede extraer información básica del dispositivo, pero también datos sensibles, como listas de contactos, registros de llamadas y la lista de cuentas de Google. Además, la aplicación es capaz de filtrar cierta información y configuraciones relacionadas con Telegram; sin embargo, estos datos no incluyen la lista de contactos de Telegram, mensajes o cualquier otra información sensible.

No obstante, si los usuarios activan una función específica de FlyGram que les permite realizar copias de seguridad y restaurar los datos de Telegram en un servidor remoto controlado por los atacantes, el actor de la amenaza tendrá acceso completo a estas copias de seguridad de Telegram, no solo a los metadatos recopilados.

Estas copias de seguridad no contienen mensajes reales. Durante el análisis de esta característica, desde ESET detectaron que el servidor asigna un ID único a cada cuenta de usuario recién creada. Este ID sigue un patrón secuencial, lo que indica que un mínimo de 13.953 cuentas de FlyGram habían activado esta función.

Signal Plus Messenger recopila datos de dispositivos e información sensible similares; su principal objetivo, sin embargo, es espiar las comunicaciones Signal de la víctima: puede extraer el número PIN de Signal que protege la cuenta Signal y hace un uso indebido de la función de enlace de dispositivos que permite a los usuarios vincular Signal Desktop y Signal iPad a sus teléfonos. Este método de espionaje destaca por su singularidad, ya que difiere de la funcionalidad de cualquier otro malware conocido.

Telemetría de detección de ESET

La telemetría de ESET informó de detecciones en dispositivos Android de Australia, Brasil, Dinamarca, República Democrática del Congo, Alemania, Hong Kong, Hungría, Lituania, Países Bajos, Polonia, Portugal, Singapur, España, Ucrania, Estados Unidos y Yemen. Además de la distribución desde la tienda oficial Google Play y Samsung Galaxy Store, las víctimas potenciales también fueron atraídas para instalar la aplicación FlyGram desde un grupo de Telegram uigur centrado en el intercambio de aplicaciones de Android, que cuenta con más de 1.300 miembros.

Como socio de Google App Defense Alliance, ESET identificó la versión más reciente de Signal Plus Messenger como maliciosa y compartió rápidamente sus hallazgos con Google. Tras su alerta, la aplicación fue eliminada de la tienda. El 27 de abril de 2023, ESET denunció Signal Plus Messenger tanto en Google Play como en Samsung Galaxy Store. Google tomó medidas y eliminó la aplicación el 23 de mayo de 2023. FlyGram fue retirada de Google Play en algún momento después del 6 de enero de 2021. Al momento, ambas aplicaciones siguen disponibles en Samsung Galaxy Store.

Puntos clave del informe:

ESET Research descubrió aplicaciones troyanizadas de Signal y Telegram para Android, llamadas Signal Plus Messenger y FlyGram, en Google Play y Samsung Galaxy Store; ambas aplicaciones fueron eliminadas posteriormente de Google Play.

El código malicioso encontrado en estas aplicaciones se atribuye a la familia de malware BadBazaar, que ha sido utilizada en el

pasado por un grupo APT alineado con China llamado GREF.

El malware BadBazaar se ha utilizado anteriormente contra uigures y otras minorías étnicas turcas. El malware FlyGram también fue visto compartido en un grupo uigur de Telegram, lo que coincide con anteriores ataques de la familia de malware BadBazaar.

FlyGram puede acceder a las copias de seguridad de Telegram si el usuario activa una función específica añadida por los atacantes; la función fue activada por al menos 13.953 cuentas de usuario.

Con información de El Impulso