Un malware para Android conocido como FireScam, diseñado para robar información confidencial, ha sido descubierto haciéndose pasar por una versión premium de la aplicación de mensajería Telegram. Su objetivo es extraer datos y mantener un control remoto continuo sobre los dispositivos afectados.

> *«Presentado como una falsa app 'Telegram Premium', se distribuye mediante un sitio de phishing alojado en GitHub.io que simula ser RuStore, una reconocida tienda de aplicaciones en Rusia»*, explicó Cyfirma, calificando esta amenaza como *«compleja y versátil».*
>
> *«El malware utiliza un proceso de infección en varias fases, comenzando con un APK introductorio, y lleva a cabo actividades avanzadas de monitoreo tras su instalación».*

El sitio de phishing en cuestión, rustore-apk.github[.]io, imita la apariencia de RuStore, una tienda de aplicaciones creada por la empresa tecnológica rusa VK. Su propósito es proporcionar un archivo APK inicial llamado «*GetAppsRu.apk*«.

Al instalarse, este APK actúa como un cargador que introduce el componente principal del malware. Este componente se encarga de sustraer información sensible, como notificaciones, mensajes y datos de otras aplicaciones, enviándola a un punto de almacenamiento en Firebase Realtime Database.

La aplicación descargadora solicita múltiples permisos, como escribir en el almacenamiento externo e instalar, modificar o eliminar aplicaciones en dispositivos Android con versión 8 o superior.

> *«El permiso ENFORCE_UPDATE_OWNERSHIP limita las actualizaciones de las aplicaciones al propietario definido de las mismas. El instalador original de una app*

> *puede designarse como 'propietario de actualizaciones', lo que le permite controlar este proceso»*, señaló Cyfirma.
> *«Este mecanismo asegura que cualquier intento de actualización por parte de otros instaladores requiera la aprobación del usuario. Al declararse como propietario de las actualizaciones, una app maliciosa puede bloquear actualizaciones legítimas, manteniendo su presencia en el dispositivo».*

FireScam emplea técnicas avanzadas de ocultamiento y anti-análisis para evitar ser detectado. Además, monitoriza notificaciones, cambios en la pantalla, transacciones de comercio electrónico, contenido del portapapeles y actividades del usuario para recopilar información de interés. Otra función destacada es su capacidad para descargar y analizar imágenes desde URLs específicas.

La falsa app Telegram Premium, al ejecutarse, solicita permisos para acceder a contactos, registros de llamadas y mensajes SMS. Posteriormente, muestra una página de inicio de sesión legítima de Telegram mediante un WebView, diseñada para capturar credenciales de acceso. Este proceso de recolección de datos se lleva a cabo independientemente de si el usuario inicia sesión o no.

El malware también registra un servicio para recibir notificaciones de Firebase Cloud Messaging (FCM), lo que le permite ejecutar comandos remotos y mantener acceso encubierto. Paralelamente, establece una conexión WebSocket con su servidor de comando y control (C2) para transferir información y realizar operaciones adicionales.

Según Cyfirma, el dominio de phishing también albergaba otro archivo malicioso denominado CDEK, que posiblemente hace referencia a un servicio ruso de seguimiento de envíos. Sin embargo, la firma no pudo obtener este archivo durante su investigación.

Aún no se ha identificado a los operadores detrás de FireScam ni cómo los usuarios llegan a los enlaces de descarga. No se sabe si utilizan técnicas como el phishing por SMS o publicidad maliciosa para atraer a las víctimas.

> *«Al imitar plataformas legítimas como la tienda RuStore, estos sitios fraudulentos aprovechan la confianza de los usuarios para engañarlos y lograr que instalen aplicaciones falsas»,* afirmó Cyfirma.
>
> «FireScam ejecuta actividades maliciosas como el robo de datos y la vigilancia, demostrando la eficacia de los métodos de distribución basados en phishing para comprometer dispositivos y eludir los sistemas de detección».