Una campaña de fraude a gran escala ha utilizado aplicaciones de trading falsas publicadas en la Apple App Store y Google Play Store, así como sitios de phishing, para engañar a las víctimas, según lo revelado por Group-IB.

Este fraude forma parte de un esquema de inversión engañosa, conocido comúnmente como *«pig butchering»* (engorde del cerdo), donde las víctimas potenciales son atraídas a invertir en criptomonedas u otros instrumentos financieros después de que los estafadores ganan su confianza haciéndose pasar por asesores de inversiones o intereses románticos.

Estas tácticas manipuladoras y de ingeniería social suelen llevar a que las víctimas pierdan sus ahorros, y en algunos casos, los delincuentes logran extraer más dinero solicitando el pago de varias tarifas y otros cargos adicionales.

La compañía con sede en Singapur indicó que esta operación tiene un alcance global, con víctimas registradas en Asia-Pacífico, Europa, Medio Oriente y África. Las aplicaciones falsas, creadas utilizando el marco UniApp, han sido denominadas UniShadowTrade.

Este grupo de actividades fraudulentas ha estado activo al menos desde mediados de 2023, atrayendo a sus víctimas con promesas de ganancias rápidas mediante aplicaciones maliciosas. Un aspecto destacado de la amenaza es que una de las aplicaciones logró pasar el proceso de revisión de la App Store de Apple, lo que le dio una apariencia de legitimidad y confianza.

La aplicación en cuestión, llamada SBI-INT, ya no está disponible para su descarga en las tiendas de aplicaciones, pero se disfrazaba como un software diseñado para *«fórmulas matemáticas algebraicas comunes y el cálculo de áreas de volumen en gráficos 3D».*

Se cree que los criminales lograron burlar los controles mediante una verificación que incluía el código fuente de la aplicación, la cual revisaba si la fecha y hora actual eran anteriores al 22 de julio de 2024, 00:00:00. Si se cumplía esta condición, la aplicación mostraba una pantalla falsa con fórmulas y gráficos.

Tras ser eliminada semanas después de su publicación, los ciberdelincuentes detrás de esta operación cambiaron su estrategia y comenzaron a distribuir la aplicación, tanto para Android como para iOS, a través de sitios de phishing.

> *«En el caso de los usuarios de iOS, al presionar el botón de descarga, se inicia la descarga de un archivo .plist, lo que hace que iOS solicite permiso para instalar la aplicación»*, explicó Andrey Polovinkin, investigador de Group-IB.
>
> *«Sin embargo, una vez completada la descarga, la aplicación no se puede abrir de*

> *inmediato. Los estafadores instruyen a la víctima para que confíe manualmente en el perfil de desarrollador empresarial. Una vez que se completa este paso, la aplicación fraudulenta se activa».*

Aquellos que terminan instalando y abriendo la aplicación se encuentran con una página de inicio de sesión, que les solicita ingresar su número de teléfono y contraseña. El proceso de registro también requiere un código de invitación, lo que sugiere que los delincuentes están dirigiendo esta estafa a individuos específicos.

Un registro exitoso pone en marcha un proceso de ataque de seis etapas en el que las víctimas son inducidas a proporcionar documentos de identidad como verificación, información personal y detalles sobre su trabajo actual. Luego, se les solicita que acepten los términos y condiciones del servicio para poder realizar las inversiones.

Después de que se ha hecho el depósito, los ciberdelincuentes envían más instrucciones sobre qué instrumento financiero utilizar, prometiendo a menudo altos rendimientos y engañando a las víctimas para que sigan invirtiendo más dinero. Para mantener el fraude, la aplicación está configurada para mostrar que las inversiones están generando beneficios.

El problema surge cuando la víctima intenta retirar sus fondos; en ese momento, se les pide que paguen tarifas adicionales para recuperar sus inversiones iniciales y las supuestas ganancias. Sin embargo, los fondos en realidad son robados y transferidos a cuentas controladas por los atacantes.

Otra estrategia innovadora utilizada por los creadores del malware es la inclusión de una configuración que especifica detalles sobre la URL que aloja la página de inicio de sesión y otros aspectos de la aplicación de inversión supuestamente legítima.

Esta configuración está alojada en una URL asociada con un servicio legítimo llamado TermsFeed, que ofrece soluciones de cumplimiento para la creación de políticas de privacidad, términos y condiciones, y banners de consentimiento de cookies.

> *«La primera aplicación descubierta, distribuida a través de la Apple App Store, actúa como un descargador, simplemente recuperando y mostrando la URL de una aplicación web. Por otro lado, la segunda aplicación, descargada de sitios de phishing, ya incluye la aplicación web en sus archivos»*, explicó Polovinkin.

Según Group-IB, este enfoque es una táctica deliberada de los atacantes para reducir las probabilidades de detección y evitar sospechas cuando la aplicación se distribuye a través de la App Store.

Además, la firma de ciberseguridad también identificó una aplicación fraudulenta de inversión en acciones en Google Play Store llamada FINANS INSIGHTS (com.finans.insights). Otra aplicación vinculada al mismo desarrollador, Ueaida Wabi, es FINANS TRADER6 (com.finans.trader).

Aunque ambas aplicaciones ya no están disponibles en Play Store, los datos de Sensor Tower indican que se descargaron menos de 5,000 veces. Japón, Corea del Sur y Camboya fueron los principales países donde se utilizó FINANS INSIGHTS, mientras que Tailandia, Japón y Chipre fueron las principales regiones para FINANS TRADER6.

> *«Los ciberdelincuentes siguen aprovechando plataformas confiables como Apple Store y Google Play para distribuir malware disfrazado de aplicaciones legítimas, explotando la confianza que los usuarios tienen en estos entornos seguros»,* afirmó Polovinkin.

> *«Las víctimas son atraídas con la promesa de obtener ganancias financieras rápidas, solo para descubrir que no pueden retirar sus fondos tras realizar grandes inversiones. El uso de aplicaciones basadas en la web también ayuda a ocultar la actividad maliciosa, lo que dificulta aún más su detección.»*