Los clientes bancarios en la región de Asia Central han sido víctimas de una nueva variante de malware para Android, denominada Ajina.Banker, desde al menos noviembre de 2024. El objetivo de este malware es robar información financiera e interceptar mensajes de autenticación de dos factores (2FA).

Group-IB, una empresa con sede en Singapur, descubrió esta amenaza en mayo de 2024. Según la compañía, el malware se propaga a través de una red de canales de Telegram creados por los atacantes, quienes se hacen pasar por aplicaciones legítimas relacionadas con servicios bancarios, sistemas de pago, servicios gubernamentales o herramientas de uso diario.

> *«El atacante cuenta con una red de afiliados interesados en obtener ganancias financieras, difundiendo malware bancario para Android que afecta a usuarios comunes»,* explicaron los investigadores de seguridad Boris Martynyuk, Pavel Naumov y Anvar Anarkulov.

Entre los países afectados por esta campaña se encuentran Armenia, Azerbaiyán, Islandia, Kazajistán, Kirguistán, Pakistán, Rusia, Tayikistán, Ucrania y Uzbekistán.

Hay indicios de que ciertos aspectos del proceso de distribución del malware a través de Telegram podrían estar automatizados para mejorar su eficacia. Se ha observado que las cuentas de Telegram creadas con este fin están diseñadas para enviar mensajes con enlaces a otros canales o fuentes externas, así como archivos APK, engañando a los destinatarios.

El uso de enlaces que redirigen a canales de Telegram con archivos maliciosos tiene la ventaja de evitar las medidas de seguridad y restricciones aplicadas en muchos chats comunitarios, permitiendo que las cuentas sigan operando sin ser bloqueadas por la moderación automática.

Además de aprovechar la confianza de los usuarios en los servicios legítimos para aumentar la tasa de infección, la táctica también implica compartir archivos maliciosos en chats locales

de Telegram, presentándolos como promociones o sorteos que prometen recompensas atractivas y acceso exclusivo a servicios.

> *«El uso de mensajes temáticos y estrategias promocionales adaptadas localmente fue especialmente efectivo en los chats comunitarios regionales. Al ajustar su enfoque a los intereses y necesidades de la población local, Ajina logró incrementar notablemente las infecciones exitosas»,* explicaron los investigadores.

También se ha detectado que los atacantes inundan los canales de Telegram con múltiples mensajes enviados simultáneamente desde diferentes cuentas, lo que indica un esfuerzo coordinado que probablemente utiliza una herramienta de distribución automatizada.

El malware es relativamente sencillo: una vez instalado, se conecta a un servidor remoto y solicita al usuario permisos para acceder a mensajes SMS, APIs de números de teléfono e información sobre la red celular.

Ajina.Banker puede recopilar datos de la tarjeta SIM, una lista de aplicaciones financieras instaladas y mensajes SMS, y luego envía esta información al servidor.

Las nuevas versiones del malware también están diseñadas para mostrar páginas de phishing, con el fin de obtener información bancaria. Además, pueden acceder a los registros de llamadas y contactos, así como abusar de la API de accesibilidad de Android para evitar ser desinstalado y obtener permisos adicionales.

> *«La contratación de programadores de Java, junto con la creación de un bot de Telegram que ofrece la oportunidad de ganar dinero, sugiere que la herramienta está en pleno desarrollo y cuenta con el apoyo de una red de afiliados»,* señalaron los investigadores.

> *«El análisis de los nombres de archivos, los métodos de distribución y otras actividades de los atacantes indica que tienen un conocimiento cultural de la región en la que operan».*

Esta revelación coincide con el descubrimiento de Zimperium sobre los vínculos entre dos familias de malware para Android conocidas como SpyNote y Gigabud (parte de la familia GoldFactory, que también incluye GoldDigger).

«Los dominios con estructuras similares (utilizando las mismas palabras clave inusuales como subdominios) y objetivos utilizados para distribuir muestras de Gigabud también se emplearon para propagar muestras de SpyNote. Este solapamiento en los métodos de distribución indica que es probable que el mismo grupo esté detrás de ambas familias de malware, lo que sugiere una campaña amplia y bien coordinada», informó la empresa.