Expertos en seguridad informática han revelado un nuevo y avanzado malware para Android denominado FjordPhantom, que ha sido detectado afectando a usuarios en países del sudeste asiático como Indonesia, Tailandia y Vietnam desde principios de septiembre de 2023.

> *«Su propagación se realiza principalmente a través de servicios de mensajería, combinando malware basado en aplicaciones con técnicas de ingeniería social para estafar a clientes bancarios»,* informó la firma de seguridad de aplicaciones móviles Promon, con sede en Oslo, en un análisis publicado el jueves.

Diseminado principalmente mediante correos electrónicos, mensajes de texto y aplicaciones de mensajería, las cadenas de ataque engañan a los destinatarios para que descarguen una supuesta aplicación bancaria que aparenta tener funciones legítimas, pero que también incorpora componentes maliciosos.

Posteriormente, las víctimas son sometidas a una técnica de ingeniería social similar a la entrega de ataques orientados a llamadas telefónicas (TOAD), que implica llamar a un falso centro de llamadas para recibir instrucciones detalladas sobre cómo ejecutar la aplicación.

Una característica distintiva de este malware, que lo diferencia de otros troyanos bancarios similares, es el uso de virtualización para ejecutar código malicioso en un contenedor y evadir la detección.

Este método astuto, según Promon, burla las protecciones de «sandbox» de Android al permitir que distintas aplicaciones se ejecuten en el mismo entorno aislado, posibilitando que el malware acceda a datos sensibles sin requerir privilegios de root.

> *«Las soluciones de virtualización, como la empleada por este malware, también pueden ser utilizadas para inyectar código en una aplicación, ya que la solución de virtualización primero carga su propio código (y todo lo demás que contiene en su*

> *aplicación) en un nuevo proceso y luego carga el código de la aplicación alojada»,* explicó el investigador de seguridad Benjamin Adolphi.

En el caso de FjordPhantom, la aplicación principal descargada contiene un módulo malicioso y el componente de virtualización, que luego se utiliza para instalar y lanzar la aplicación incrustada del banco objetivo en un contenedor virtual.

En otras palabras, la aplicación fraudulenta está diseñada para cargar la aplicación legítima del banco en un contenedor virtual, mientras utiliza un marco de interceptación dentro del entorno para modificar el comportamiento de las API clave y obtener información sensible de la pantalla de la aplicación de forma programática, cerrando además cuadros de diálogo que alertan sobre actividades maliciosas en los dispositivos de los usuarios.

> Consultado para obtener comentarios, un portavoz de Google informó que *«los usuarios están protegidos por Google Play Protect, que puede advertir a los usuarios o bloquear aplicaciones conocidas por exhibir comportamientos maliciosos en dispositivos Android con Google Play Services, incluso cuando esas aplicaciones provienen de fuentes fuera de Google Play».*

> *«FjordPhantom en sí mismo está programado de manera modular para atacar diferentes aplicaciones bancarias. Dependiendo de la aplicación bancaria que esté incrustada en el malware, se llevarán a cabo diversos ataques contra estas aplicaciones»,* señaló Adolphi.