Microsoft detalló las capacidades en evolución de las aplicaciones de malware de fraude telefónico en Android, señalando su *«flujo de ataque complejo de varios pasos»* y un mecanismo mejorado para evadir el análisis de seguridad.

El fraude telefónico pertenece a una categoría de fraude de facturación en la que las aplicaciones móviles maliciosas vienen con tarifas de suscripción ocultas, lo que atrae a los usuarios desprevenidos a contenido premium sin su conocimiento o consentimiento.

También se diferencia de otras amenazas de fleeceware en las que las funciones maliciosas solo se llevan a cabo cuando un dispositivo comprometido se conecta a uno de sus operadores de red objetivo.

> *«También, de forma predeterminada, utiliza la conexión celular para sus actividades y obliga a los dispositivos a conectarse a la red móvil aún si hay una conexión WiFi disponible»,* dijeron Dimitrios Valsamaras y Sang Shin Jung, del Microsoft 365 Defender Reseach Team.

> *«Una vez que se confirma la conexión a una red de destino, sigilosamente inicia una suscripción fraudulenta y la confirma sin el consentimiento del usuario, en algunos casos incluso interceptando la contraseña de un solo uso (OTP) para hacerlo».*

También se sabe que dichas aplicaciones suprimen las notificaciones por SMS relacionadas con la suscripción para evitar que las víctimas se den cuenta de la transacción fraudulenta y se den de baja del servicio.

En esencia, el fraude telefónico se aprovecha del método de pago que permite a los consumidores suscribirse a servicios pagos desde sitios web compatibles con el Protocolo de Aplicación Inalámbrica (WAP). Esta cuota de suscripción de carga de forma directa en la factura del teléfono móvil de los usuarios, evitando así la necesidad de configurar una tarjeta

de crédito o débito o ingresar un nombre de usuario y contraseña.

> *«Si el usuario se conecta a Internet por medio de datos móviles, el operador de la red móvil puede identificarlo por dirección IP. Los operadores de redes móviles cobran a los usuarios solo si se identifican con éxito»,* dijo Kapsersky en un informe de 2017 sobre los troyanos de facturación WAP.

De forma opcional, algunos proveedores también pueden requerir OTP como una segunda capa de confirmación de la suscripción antes de activar el servicio.

> *«En el caso del fraude telefónico, el malware realiza la suscripción en nombre del usuario de una forma que no se percibe el proceso general. El malware se comunicará con un servidor para recuperar una lista de los servicios ofrecidos»,* dijeron los investigadores.

Se logra apagando primero el WiFi y activando los datos móviles, después haciendo uso de JavaScript para suscribirse sigilosamente al servicio e interceptando y enviando el código OTP (si corresponde) para completar el proceso.

El código JavaScript, por su parte, está diseñado para hacer clic en elementos HTML que contienen palabras clave como *«confirmar», «hacer clic» y «continuar»* para iniciar la suscripción mediante programación.

Después de una suscripción fraudulenta exitosa, el malware oculta los mensajes de notificación de suscripción o abusa de sus permisos de SMS para eliminar los mensajes de texto entrantes que contienen información sobre el servicio suscrito del operador de red móvil.

También se sabe que el malware de fraude de llamadas encubre su comportamiento

malicioso por medio de la carga dinámica de código, una función en Android que permite que las aplicaciones extraigan módulos adicionales de un servidor remoto durante el tiempo de ejecución, lo que lo hace propicio para el abuso por parte de los atacantes.

Desde el punto de vista de la seguridad, esto también significa que un autor de malware puede diseñar una aplicación de tal forma que la funcionalidad maliciosa solo se cargue cuando se cumplan ciertos requisitos previos, lo que anula de forma efectiva las comprobaciones de análisis de código estático.

«Si una aplicación permite la carga dinámica de código y el código cargado dinámicamente extrae mensajes de texto, se clasificará como malware de puerta trasera», establece Google en su documentación para desarrolladores sobre aplicaciones potencialmente dañinas (PHA).

Con una tasa de instalación del 0.022%, las aplicaciones de fraude telefónico representaron el 34.8% de todas las PHA instaladas desde el mercado de aplicaciones de Android en el primer trimestre de 2022, ocupando el segundo lugar por debajo del spyware. La mayoría de las instalaciones procedían de India, Rusia, México, Indonesia y Turquía.

Para mitigar la amenaza del malware de fraude telefónico, se recomienda que los usuarios instalen aplicaciones solo desde Google Play Store u otras fuentes confiables, eviten otorgar permisos excesivos a las aplicaciones y consideren actualizar a un nuevo dispositivo en caso de que deje de recibir actualizaciones de software.