Los investigadores de seguridad cibernética publicaron este lunes los detalles de un nuevo troyano para Android que aprovecha las funciones de accesibilidad en los dispositivos móviles para desviar las credenciales de los servicios bancarios y de criptomonedas en Italia, Reino Unido y Estados Unidos.

Nombrado como SharkBot por Cleafy, el malware está diseñado para atacar un total de 27 objetivos, contando 22 bancos internacionales no identificados en Italia y Reino Unido, así como cinco aplicaciones de criptomonedas en Estados Unidos al menos desde finales de octubre de 2021. Se cree que el malware se encuentra en sus primeras etapas de desarrollo, sin superposiciones con ninguna familia conocida.

> *«El objetivo principal de SharkBot es iniciar transferencias de dinero desde los dispositivos comprometidos a través de la técnica de Sistemas de Transferencia Automática (ATS) sin pasar por los mecanismos de autenticación de múltiples factores, como SCA»,* dijeron los investigadores.
>
> *«Una vez que SharkBot se instala con éxito en el dispositivo de la víctima, los atacantes pueden obtener información bancaria confidencial mediante el abuso de los Servicios de Accesibilidad, como credenciales, información personal, saldo actual, etc.., pero también para realizar gestos en el dispositivo afectado».*

Enmascarado como reproductor multimedia, televisión en vivo o aplicaciones de recuperación de datos, SharkBot, al igual que sus homólogos de malware TeaBot y ubel, pide de forma repetida a los usuarios permisos en ventanas emergentes con el fin de robar información sensible.

Lo que destaca de esta campaña es la explotación de la configuración de accesibilidad para llevar a cabo ataques ATS, que permiten a los operadores *«autocompletar campos en aplicaciones legítimas de banca móvil e iniciar transferencias de dinero desde los dispositivos comprometidos a una red de mulas de dinero controlada por el actor de amenazas».*

El modus operandi efectivamente elimina la necesidad de registrar un nuevo dispositivo para realizar actividades fraudulentas, mientras que también pasa por alto los mecanismos de autenticación de dos factores implementados por las aplicaciones bancarias.

Además, el malware viene con varias características que ahora se observan en todos los troyanos bancarios de Android, como la capacidad de realizar ataques de superposición para robar credenciales de inicio de sesión e información de tarjetas de crédito, interceptar comunicaciones bancarias legítimas enviadas a través de SMS, habilitar el registro de teclas y obtener un control remoto completo de los dispositivos comprometidos.

SharkBot también se destaca por los pasos que toma para evadir el análisis y la detección, incluida la ejecución de comprobaciones del emulador, el cifrado de las comunicaciones de comando y control con un servidor remoto y la ocultación del icono de la aplicación en la pantalla de inicio después de la instalación.

Hasta ahora no se han detectado muestras del malware en la tienda Google Play, lo que implica que las aplicaciones maliciosas se instalan en los dispositivos de los usuarios, ya sea a través de sistemas de descarga lateral o de ingeniería social.

El descubrimiento de SharkBot en la naturaleza muestra *«cómo los malwares móviles están encontrando rápidamente nuevas formas de realizar fraudes, tratando de eludir las contramedidas de detección de comportamiento implementadas por múltiples bancos y servicios financieros durante los últimos años»,* dijeron los investigadores.