El troyano bancario para Android conocido como SharkBot volvió a aparecer en Google Play Store haciéndose pasar por aplicaciones antivirus y de limpieza de archivos.

> *«Este nuevo cuentagotas no depende de los permisos de Accesibilidad para realizar automáticamente la instalación del malware cuentagotas Sharkbot. En cambio, esta nueva versión pide a la víctima que instale el malware como una actualización falsa para que el antivirus permanezca protegido contra las amenazas»,* dijo Fox-IT de NCC Group.

Las aplicaciones en cuestión, Mister Phone Cleaner y Kylhavy Mobile Security, cuentan con más de 60,000 instalaciones entre ellas y están diseñadas para usuarios de España, Australia, Polonia, Alemania, Estados Unidos y Austria.

- Mister Phone Cleaner (com.mbkristine8.cleanmaster, más de 50 000 descargas)
- Kylhavy Mobile Security (com.kylhavy.antivirus, más de 10 000 descargas)

Los cuentagotas están diseñados para lanzar una nueva versión de SharkBot, denominada V2 por la empresa de seguridad holandesa ThreatFabric, que cuenta con un mecanismo de comunicación de comando y control (C2) actualizado, un algoritmo de generación de dominio (DGA) y una base de código completamente refactorizada.

Fox-IT dijo que descubrió una nueva versión 2.25 el 22 de agosto de 2022, que presenta una función para desviar cookies cuando las víctimas inician sesión en sus cuentas bancarias, al mismo tiempo que elimina la capacidad de responder de forma automática a los mensajes entrantes con enlaces al malware para su propagación.

Al evitar los permisos de Accesibilidad para instalar SharkBot, el desarrollo destaca que los operadores están modificando activamente sus técnicas para evitar la detección, sin mencionar la búsqueda de métodos alternativos frente a las restricciones recientemente impuestas por Google para reducir el abuso de las API.

Otras capacidades notables de robo de información incluyen la inyección de superposiciones falsas para recopilar credenciales de cuentas bancarias, el registro de pulsaciones de teclas, la interceptación de mensajes SMS y la realización de transferencias de fondos fraudulentas usando el Sistema de Transferencia Automatizado (ATS).

No sorprende que el malware represente una amenaza omnipresente y en constante evolución, y a pesar de los continuos esfuerzos por parte de Apple y Google, las tiendas de aplicaciones son vulnerables al abuso sin saberlo para su distribución, y los desarrolladores de las aplicaciones intentan todos los trucos para eludir la seguridad.

> *«Hasta ahora, los desarrolladores de SharkBot parecen haberse centrado en el cuentagotas para seguir usando Google Play Store para distribuir su malware en las últimas campañas»,* dijeron los investigadores Alberto Segura y Mike Stokkel.