



Los operadores detrás de [BRATA](#) una vez más agregaron capacidades al malware móvil de Android en un intento de hacer que sus ataques contra las aplicaciones financieras sean más sigilosos.

*«De hecho, el modus operandi ahora encaja en un patrón de actividad de Amenaza Persistente Avanzada (APT). Este término se utiliza para describir una campaña de ataque en la que los ciberdelincuentes establecen una presencia a largo plazo en una red específica para robar información confidencial»,* [dijo](#) la compañía de seguridad Cleafy.

Acrónimo de «Brazilian Remote Access Tool Android» BRATA se detectó por primera vez en estado salvaje en Brasil a fines de 2018, antes de hacer su primera aparición en Europa en abril pasado, mientras se hacía pasar por software antivirus y otras herramientas de productividad comunes para engañar a los usuarios para que las descargaran.

El cambio en el patrón de ataque, que escaló nuevos máximos a inicios de abril de 2022, implica adaptar el malware para atacar una institución financiera específica a la vez, cambiando a un banco diferente solo después de que la víctima comience a implementar contramedidas contra la amenaza.

Las aplicaciones no autorizadas también incorporan nuevas características que le permiten hacerse pasar por la página de inicio de sesión de la institución financiera para recopilar credenciales, acceder a mensajes SMS y transferir una carga útil de segunda etapa («unrar.jar») desde un servidor remoto para registrar eventos en el dispositivo comprometido.

*«La combinación de la página de phishing con la posibilidad de recibir y leer los SMS de la víctima podría usarse para realizar un ataque completo de adquisición de cuenta (ATO)»,* dijeron los investigadores.



Además, Cleafy dijo que encontró una muestra de paquete de aplicación de Android específica separada («SMSAppSicura.apk») que usaba la misma infraestructura de comando y control (C2) que BRATA para desviar mensajes SMS, lo que indica que los atacantes están probando distintos métodos para ampliar su alcance.

Se cree que la aplicación de robo de SMS identifica específicamente a los usuarios en Reino Unido, Italia y España, y su objetivo es poder interceptar y filtrar todos los mensajes entrantes relacionados con contraseñas de un solo uso enviadas por los bancos.

*«Las primeras campañas de malware se distribuyeron por medio de antivirus falsos u otras aplicaciones comunes, mientras que durante las campañas el malware se convierte en un ataque APT contra el cliente de un banco italiano específico»*, dijeron los investigadores.

*«Por lo general, se enfocan en entregar aplicaciones maliciosas dirigidas a un banco específico durante un par de meses y luego pasar a otro objetivo».*