Publicado en Ciudad de México el 22/11/2017

# [Un troyano de banca móvil se filtró en Google Play para dirigirse a usuarios de Citibank, BBVA y Santander](http://www.notasdeprensa.es)

## La banca móvil se basa en la conveniencia y la confianza, los usuarios exigen una experiencia segura e ininterrumpida. La aplicación de banca móvil y la tienda desde la cual se descarga deben tener políticas de seguridad que garanticen la máxima protección de los consumidores

 Avast, el líder mundial en productos de seguridad digital, dio a conocer los resultados de una encuesta realizada a más de 100 visitantes de la feria comercial Mobile World Congress Americas en la que el 71.8% de ellos cree que su dinero y transacciones de banca movil está protegido. La banca móvil se basa en la conveniencia y la confianza, y los usuarios exigen una experiencia segura e ininterrumpida. La aplicación de banca móvil y la tienda desde la cual se descarga deben tener políticas de seguridad que garanticen la máxima protección de los consumidores. Sin embargo, a veces los ciberdelincuentes logran eludir estas defensas y robar el dinero de la gente. Hace poco, el equipo de investigación de amenazas móviles de Avast trabajó en colaboración con investigadores de ESET y SfyLabs para examinar una nueva versión de BankBot, un malware que ataca la banca móvil. Este se filtró en Google Play varias veces este año, y afectó a grandes bancos, entre ellos Wells Fargo, Chase, BBVA, Santander y BNP Paribas, DiBa y Citibank, y a sus usuarios en Estados Unidos, Australia, Alemania, los Países Bajos, Francia, Polonia, España, Portugal, Turquía, Grecia, Rusia, República Dominicana, Singapur y Filipinas. Estas nuevas versiones de malware de banca móvil primero aparecieron como aplicaciones de linternas, y luego como juegos de solitario y una aplicación de limpieza, todos supuestamente confiables, y así lograron engañar a los usuarios para que las descargaran. Sin embargo, en vez de brindarles luz, alegría y comodidad, estas aplicaciones tienen oscuras intenciones, tales como espiar a las personas, recolectar sus datos bancarios y robar su dinero. Anteriormente, Google había eliminado versiones previas de BankBot del Play Store en cuestión de días. Sin embargo, varias versiones siguieron activas hasta el 17 de noviembre. Esto bastó para que infectaran miles de dispositivos. Google tiene medidas de monitoreo y verificación de todas las aplicaciones que se envían al Play Store para garantizar que no ingresen programas maliciosos. Pero en sus últimas campañas, los creadores de los troyanos bancarios han implementado técnicas especiales para eludir la detección automática de Google, y así pueden iniciar las actividades maliciosas dos horas después de que el usuario le da derechos de administrador del dispositivo a la aplicación. Además, publican las aplicaciones bajo distintos nombres de desarrollador, una técnica habitual para eludir los controles de Google. Las actividades maliciosas incluyen la instalación de una interfaz falsa colocada sobre la aplicación bancaria limpia cuando el usuario la abre. Apenas ingresa los datos bancarios, estos son recogidos por el delincuente. En algunos países, se emplean números de autenticación de las transacciones (TAN, por sus siglas en inglés), una forma de autenticación de dos factores necesaria para ejecutar transferencias en línea que suelen utilizar los bancos europeos. Los autores de BankBot interceptan los mensajes de texto de sus víctimas que traen los números TAN, lo que les permite ejecutar transacciones bancarias en nombre del usuario. Nikolaos Chrysaidos, Director de Seguridad e Inteligencia de Amenazas Móviles de Avast, afirmó: "Una nueva versión del virus troyano BankBot, que ataca la banca móvil, se filtró en Google Play en octubre y noviembre, disimulado como aplicaciones de linternas, juegos y de limpieza. Los ciberdelincuentes han atacado a los clientes de grandes bancos como Wells Fargo, Chase y alrededor de otras 160 aplicaciones bancarias de Estados Unidos, Latinoamérica, Europa y la región de Asia-Pacífico. Google suele eliminar rápidamente los programas maliciosos de Google Play, pero el problema es que las aplicaciones infectadas con el troyano BankBot hayan podido eludir los controles de seguridad de Google en primer lugar. Es fundamental que los usuarios instalen una aplicación de seguridad en sus teléfonos para protegerse de BankBot y otros troyanos bancarios. También deben tener cuidado al usar la aplicación de su banco y observar si hay modificaciones extrañas en la interfaz. Además, se les recomienda agregar una capa adicional de seguridad con autenticación de dos factores para iniciar la sesión, y solo confiar en tiendas de aplicaciones probadas para descargar estos programas. Si bien el malware se filtró en Google Play, el segundo componente, la carga de malware, se descargó de una fuente externa." Se recomienda que los usuarios sigan los siguientes pasos para protegerse de los troyanos que atacan la banca móvil: Controlar que utilicen aplicaciones bancarias verificadas. Si la interfaz tiene un aspecto diferente o extraño, volver a verificar con el equipo de atención al cliente del banco. Si el banco ofrece la opción de autenticación de dos factores, lo mejor es usarla. Solo confiar en tiendas de aplicaciones probadas, tales como Google Play o App Store de Apple. Si bien el malware se filtró en Google Play, la carga de malware se descargó de una fuente externa. Si se desactiva la opción de descargar aplicaciones de otras fuentes, no hay riesgo de que este tipo de troyanos bancarios se active en sus teléfonos. Antes de descargar una aplicación nueva, observar las calificaciones de otros usuarios. Si se quejan de una mala experiencia, tal vez sea mejor evitar esa aplicación. Prestar atención a los permisos que solicita una aplicación. Si una linterna pide permiso de acceso a los contactos, fotos o archivos multimedia, considerarlo una señal de alarma. Utilizar una aplicación de seguridad como Avast Mobile Security o AVG Antivirus para Android, que detecta BankBot y los protege. Avast (www.avast.com), líder global en productos de seguridad digital, protege a más de 400 millones de personas online. Avast ofrece productos bajo las marcas Avast y AVG que protegen a las personas de las amenazas en internet y del escenario de amenazas de Internet de las Cosas en constante evolución. La red de detección de amenazas de la compañía se encuentra entre las más avanzadas en el mundo, utilizando tecnologías de aprendizaje automático e inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital de Avast para Móvil, PC o Mac están mejor clasificados y certificados por V-100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs, entre otros. Avast cuenta con el respaldo de las principales firmas globales de capital privado CVC Capital Partners y Summit Partners.

**Datos de contacto:**

Flor Carreno

Marketing Q S SA de CV

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/un-troyano-de-banca-movil-se-filtro-en-google](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Nacional Finanzas E-Commerce Ciberseguridad Consumo



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)