Los ciberdelincuentes están aprovechando la tecnología WebAPK de Android para engañar a usuarios desprevenidos y lograr que instalen aplicaciones web maliciosas en sus teléfonos Android, diseñadas para capturar información personal confidencial.

> *«El ataque comenzó con las víctimas recibiendo mensajes de texto SMS que sugieren la necesidad de actualizar una aplicación de banca móvil. El enlace incluido en el mensaje dirigía a un sitio que utilizaba la tecnología WebAPK para instalar una aplicación maliciosa en el dispositivo de la víctima»*, informaron investigadores de CSIRT KNF en un análisis publicado la semana pasada.

La aplicación se hace pasar por PKO Bank Polski, una compañía multinacional de servicios financieros y bancarios con sede en Varsovia. Los detalles de esta campaña fueron compartidos inicialmente por una firma de ciberseguridad polaca llamada RIFFSEC.

WebAPK permite a los usuarios instalar aplicaciones web progresivas (PWAs) en la pantalla principal de sus dispositivos Android sin necesidad de recurrir a la tienda de Google Play.

> *«Cuando un usuario instala una PWA desde Google Chrome y utiliza WebAPK, el servidor de «empaquetado» genera y firma un APK para esa PWA»*, explica Google en su documentación.

> *«Este proceso toma tiempo, pero una vez que el APK está listo, el navegador instala silenciosamente la aplicación en el dispositivo del usuario. Dado que el APK está firmado por proveedores de confianza (Play Services o Samsung), el teléfono lo instala sin deshabilitar la seguridad, al igual que con cualquier otra aplicación proveniente de la tienda oficial. No es necesario instalar la aplicación desde fuentes no verificadas».*

Una vez instalada, la aplicación falsa de banca (*«org.chromium.webapk.a798467883c056fed_v2»*) insta a los usuarios a ingresar sus credenciales y tokens de autenticación de doble factor (2FA), lo que resulta en el robo efectivo de dicha información.

> *«Uno de los desafíos para enfrentar este tipo de ataques es el hecho de que las aplicaciones WebAPK generan nombres de paquetes y sumas de verificación distintos en cada dispositivo. Estos se generan dinámicamente mediante el motor de Chrome, lo que dificulta el uso de esta información como Indicadores de Compromiso (IoC)»,* mencionó CSIRT KNF.

Para contrarrestar estas amenazas, se recomienda bloquear los sitios web que utilizan el mecanismo WebAPK para llevar a cabo ataques de phishing.

Este desarrollo surge a medida que Resecurity reveló que los ciberdelincuentes están cada vez más utilizando herramientas especializadas de suplantación de dispositivos para Android, que se comercializan en la web oscura, con el propósito de hacerse pasar por titulares de cuentas comprometidas y eludir los controles de prevención de fraude.

Las herramientas de anti-detección, incluyendo Enclave Service y MacFly, son capaces de falsificar las huellas digitales de dispositivos móviles y otros parámetros de software y red que son analizados por los sistemas de prevención de fraude, y los actores malintencionados también aprovechan controles de fraude débiles para realizar transacciones no autorizadas a través de teléfonos inteligentes mediante el uso de malware bancario como TimpDoor y Clientor.

> *«Los ciberdelincuentes emplean estas herramientas para acceder a cuentas*

> *comprometidas e imitar a clientes legítimos al explotar archivos de cookies robados, suplantar identificadores de dispositivos altamente específicos y aprovechar la configuración de redes única de las víctimas de fraude»,* explicó la compañía de ciberseguridad.