KASPERSKY FRAUD PREVENTION SDK FOR MOBILE

Kaspersky Fraud Prevention SDK for Mobile es una completa solución para proteger las aplicaciones bancarias móviles que se ejecutan en Android, iOS y Windows Phone. Combina las tecnologías de seguridad de IT líderes del sector de Kaspersky Lab para proteger la información de las cuentas de los clientes, proteger las comunicaciones con el banco y garantizar que no haya amenazas que acechen en el dispositivo móvil utilizado para la banca móvil.

Kaspersky Fraud Prevention SDK for Mobile es muy flexible, lo que permite al banco trasladar sin problemas la experiencia del usuario a los dispositivos móviles de los clientes al tiempo que les ofrece protección fiable contra el fraude.

Kaspersky Fraud Prevention SDK incluye cinco áreas de funcionalidad clave para detener las adquisiciones de cuentas, inyecciones de malware y otros ataques antes de que puedan provocar daños:

ANÁLISIS Y ELIMINACIÓN DE MALWARE

Para realizar operaciones bancarias de forma segura, es fundamental contar con un dispositivo limpio y seguro. Incluso antes de que se cargue una aplicación bancaria, Kaspersky Fraud Prevention SDK se asegura de que el entorno de trabajo esté libre de malware y vulnerabilidades que podrían poner en riesgo la seguridad.

AMENAZAS

- Malware que infecta un dispositivo, antes o después de cargar la aplicación bancaria.

PROTECCIÓN

- Antes de instalar la aplicación principal, un análisis completo de malware y de vulnerabilidades detecta las posibles amenazas y permite su eliminación. Si el usuario rechaza eliminar el código malicioso detectado, se recomienda bloquear la aplicación bancaria.
- El componente antivirus protege el dispositivo en tiempo real y puede realizar análisis a petición de cualquier software instalado.

DETECCIÓN DE RIESGOS

Para garantizar la seguridad del entorno de trabajo antes de acceder a las aplicaciones bancarias, Kaspersky Fraud Prevention SDK comprueba si existen riesgos asociados con el dispositivo y su conexión a Internet.

AMENAZAS

- Dispositivos liberados y la presencia de versiones no oficiales u obsoletas de firmware que tienen vulnerabilidades sin parches.
- Redes Wi-Fi sin acreditación.
- Aplicaciones que son o podrían ser maliciosas.

PROTECCIÓN

- Comprobación de los componentes especiales para privilegios de usuarios escalados en el dispositivo y verificación de que todo el firmware se está ejecutando en su versión más actualizada.
- El análisis de seguridad de Wi-Fi confirma que el usuario está conectado a una red Wi-Fi fiable.
- La detección de riesgos alerta a la aplicación bancaria de la presencia de aplicaciones sospechosas o peligrosas. La aplicación puede advertir a los usuarios y ayudarles a eliminar el software sospechoso. Si el programa sospechoso se considera como de "alto riesgo", la aplicación bancaria se puede bloquear hasta que el peligro se elimine del dispositivo.
- La huella del dispositivo permite a la aplicación bancaria analizar información clave sobre el dispositivo (IMEI, IMSI, ubicación, número de teléfono, etc.) dentro de sus propios sistemas antifraude.

PROTECCIÓN DE NAVEGADORES MÓVILES

La mayoría de operaciones bancarias online requiere acceso a Internet, lo que significa que necesitan mecanismos que puedan proteger el intercambio de datos entre el dispositivo del usuario y el sistema bancario online.

AMENAZAS

- Phishing y sitios comprometidos.
- Falsificación de DNS, un ataque del tipo "Man-in-the-Middle" (MitM) que redirige el tráfico al servidor del atacante.
- Intercepción y modificación de información entre el dispositivo móvil y la infraestructura mediante certificados falsos o canales Wi-Fi vulnerados.

PROTECCIÓN

- Los componentes de filtrado web y URL comprueban la reputación de los recursos en una base de datos en la nube. El componente de antivirus web comprueba si el cuerpo de la página web contiene algún código malicioso. Los recursos no seguros se bloquean y se le notifica al usuario.
- El comprobador de DNS confirma que este dominio coincide con dirección IP fiable del banco. Si existe alguna discrepancia, la sesión bancaria se da por finalizada y se alerta al usuario del problema.
- El componente de validación de certificados confirma la autenticidad del servidor al que se ha conectado. Se comprueban las conexiones Wi-Fi para asegurarse de que están cifradas.

PROTECCIÓN DE DATOS Y SMS

Cualquier sistema bancario online necesita compartir información importante con sus usuarios. Estos datos pueden ser vulnerables cuando se envían desde el banco al usuario o desde el usuario al banco. Kaspersky Fraud Prevention SDK ofrece protección en este caso.

AMENAZAS

- Syware que graba pulsaciones y transmite esta información a los cibercriminales, lo que permite el acceso potencial a las credenciales de inicio de sesión.
- Intercepción y falsificación de mensajes SMS entre el banco y el usuario, lo que permite que los cibercriminales accedan a información confidencial o manipulen una transacción.
- Aplicaciones maliciosas que pueden acceder a datos importantes en el dispositivo del usuario.

PROTECCIÓN

- Se utiliza un teclado seguro y campos de entrada seguros para proteger la introducción de todos los datos confidenciales.
- El SMS seguro reconoce e intercepta cualquier mensaje del banco. Los mensajes se pueden eliminar del buzón de entrada y se almacenan de forma segura en otro lugar.
- El almacenamiento seguro proporciona un área protegida para almacenar los datos confidenciales.

AUTODEFENSA

Las funciones incorporadas garantizan que el malware no pueda interferir en el funcionamiento de Kaspersky Fraud Prevention SDK.

AMENAZAS

- Intentos de descargar software de seguridad de IT del dispositivo, dejándolo vulnerable a los ataques.
- Modificaciones en los recursos o el código binario de la aplicación basada en SDK.
- Bases de datos de antivirus obsoletas que dejan el dispositivo abierto a ataques de malware descubierto después de la última actualización.

PROTECCIÓN

- Kaspersky Fraud Prevention SDK incluye un mecanismo que impide que el malware bloquee sus tecnologías de protección.
- Hay cinco medios para impedir modificaciones:
  - Aplicar el certificado digital de la aplicación basada en SDK, y ejecutar una comprobación de integridad
  - El relanzamiento de la aplicación si se detiene
  - Proteger la aplicación principal en tiempo real
  - Detectar métodos de inyección
  - Desactivar el modo de depuración
- La herramienta del actualizador actualiza los componentes de antivirus al menos una vez cada 24 horas, y asegura que se actualicen antes de utilizar la aplicación bancaria

Kaspersky Lab también ofrece todo el soporte necesario durante el proceso de implementación. Nuestro equipo de servicios profesionales está accesible en todo momento para asesorar sobre la mejor forma de poner en marcha Kaspersky Fraud Prevention – SDK, garantizando que la instalación pueda gestionarse con rapidez y fluidez.

Marzo de 2015/Global

KASPERSKY lab