KASPERSKY FRAUD PREVENTION FOR ENDPOINTS

KASPERSKY lab

www.kaspersky.es

KASPERSKY FRAUD PREVENTION

1. Formas de atacar a la banca online

El primer motivo del cibercrimen es hacer dinero y las sofisticadas bandas criminales de hoy en día disponen de una amplia variedad de técnicas que les ayudan a robar a los bancos online y los servicios financieros. Tanto si se trata de malware para manipular las transacciones legítimas y desviar el dinero a sus propias cuentas, o una combinación de ingeniería social y phishing para obtener acceso a las cuentas, los cibercriminales se sirven de varios métodos para robar a los usuarios de los servicios de banca online.

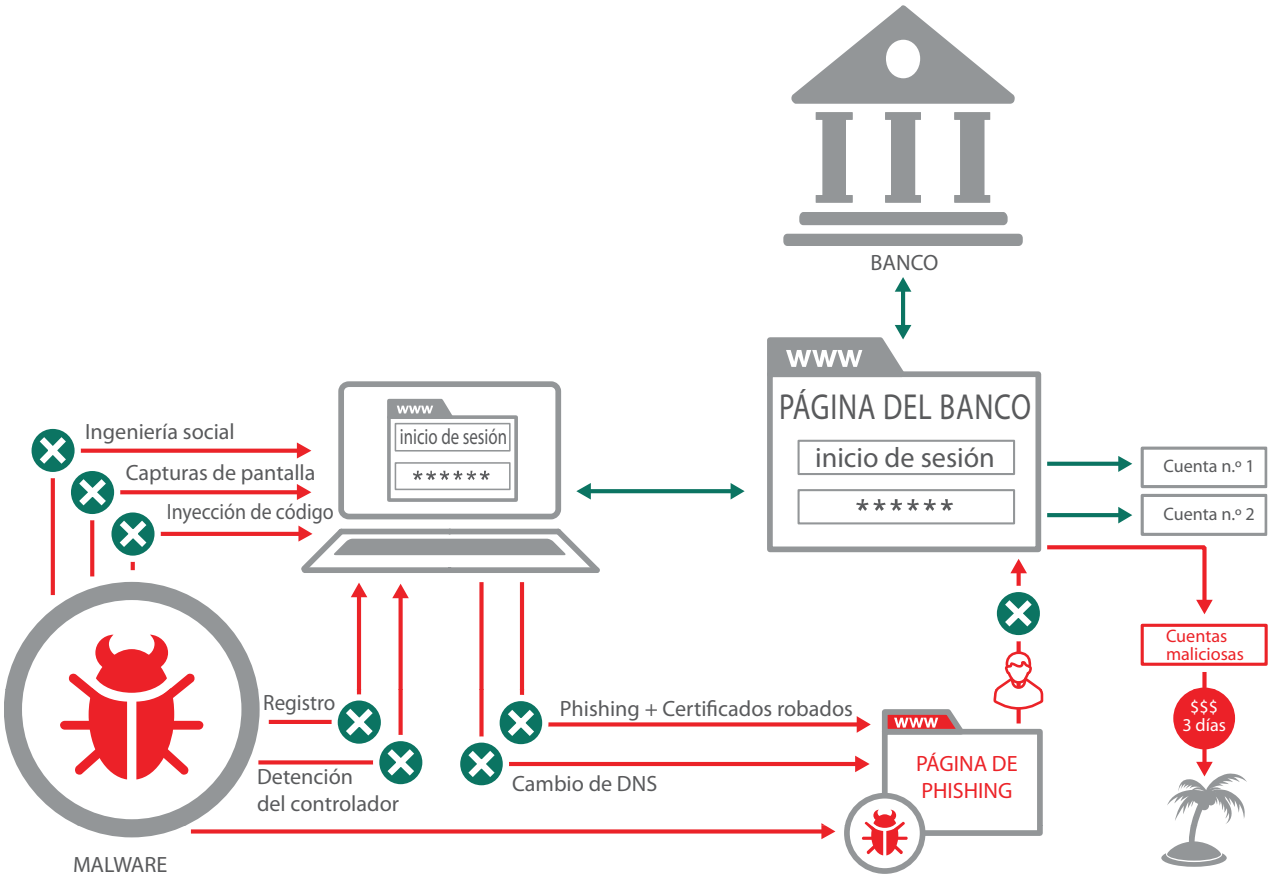
Hay dos amenazas principales:

- Adquisición de cuentas, que consiste en robar las credenciales de un usuario y utilizarlas para sacar dinero de la cuenta
- Manipulación de transacciones, que consiste en cambiar los detalles de la transacción o crear una nueva transacción en nombre del cliente

Kaspersky Fraud Prevention for Endpoints protege contra las siguientes amenazas:

- Robo de credenciales
  - Phishing
  - Ingeniería social
  - Fuga de datos
  - Modificación de páginas web (introducción web)
  - Form Grabbing
  - Keylogging
  - Capturas de pantalla
  - Ataques de falsificación
- Manipulación de transacciones
  - Ataques del tipo "Man-in-the-Middle" (MitM)
  - Acceso remoto
  - Ataques del tipo "Man-in-the-Browser" (MitB)

2. Fraud Prevention en acción



3. Tecnologías de protección

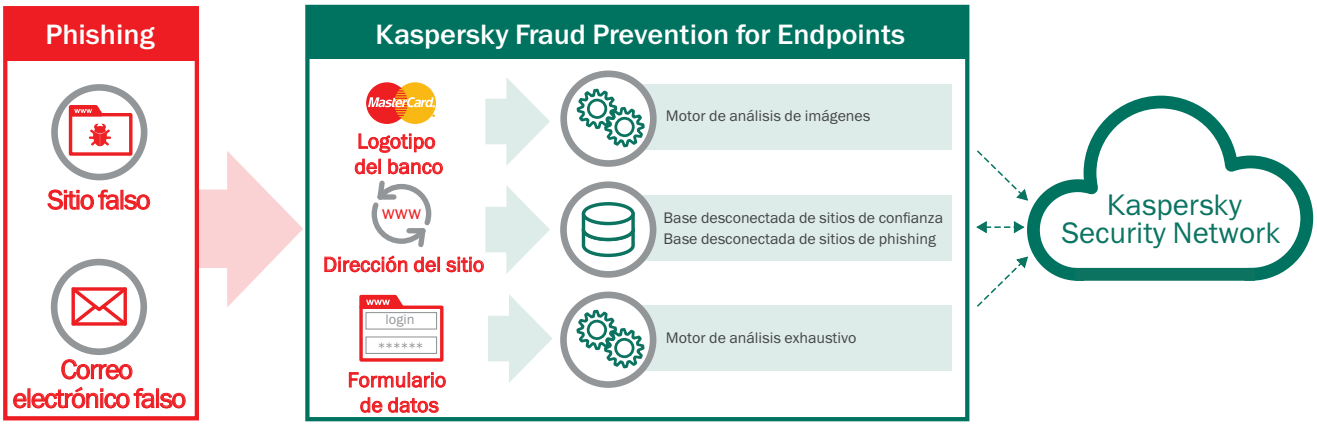
3.1 Antiphishing

El sistema antiphishing de Kaspersky Lab combina análisis exhaustivos y tecnologías en la nube con bases de datos desconectadas tradicionales para garantizar que se bloquean incluso las amenazas nuevas y desconocidas.

El módulo antiphishing de actualización rápida en la nube contiene máscaras de URL de phishing. Las nuevas amenazas se pueden añadir a los pocos segundos de su detección, ofreciendo así a sus ordenadores protección contra sitios de phishing que aún no están incluidos en las bases de datos locales. Cada vez que el usuario encuentra una URL que no está en la base local, el sistema lo comprueba automáticamente en la nube.

El componente web exhaustivo del sistema antiphishing se activa cuando el usuario hace clic en un enlace a una página web de phishing que aún no se ha incluido en las bases de datos de Kaspersky Lab.

Además, una amplia base de datos sin conexión antiphishing, almacenada en los dispositivos de los usuarios, contiene todas las máscaras más generalizadas de URL de phishing.



3.2 Análisis de malware y eliminación

Incluso si ya hay malware en el equipo de un usuario, Kaspersky Fraud Prevention aún puede proteger las operaciones bancarias online. En el momento de la instalación, Kaspersky Fraud Prevention realiza un análisis del sistema para encontrar malware de banca. Se alerta a los usuarios de los posibles problemas y se les invita a eliminar los archivos maliciosos y desinfectar el equipo. La solución ejecuta un análisis adicional cada vez que el navegador de la banca protegido se inicia.

ESTUDIO DE CASO

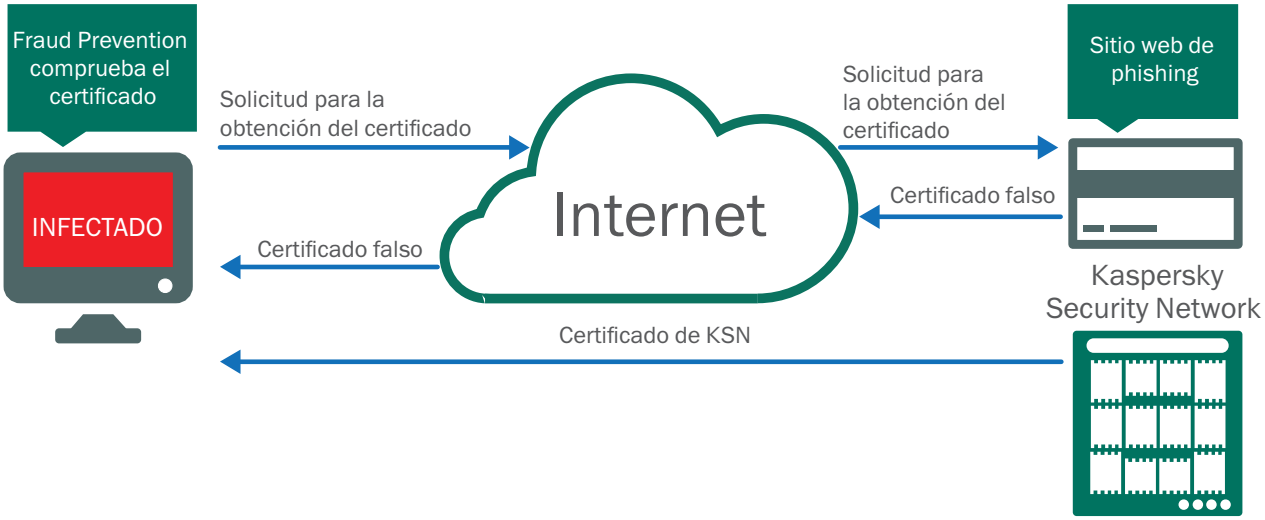
Un gran banco ruso estaba bajo amenaza por un elemento de malware que redirigía automáticamente a sus clientes a una página de phishing. De esta forma, no solo redirigía a los usuarios engañados para que entregaran sus credenciales bancarias a los cibercriminales, sino que también hizo que no pudieran volver a acceder a la página real del banco en el futuro. Kaspersky Fraud Prevention eliminó correctamente el malware en los ordenadores de los clientes, asegurando que pudieran realizar operaciones bancarias online con total seguridad en el futuro.

Kaspersky Fraud Prevention for Endpoints es compatible con todas las aplicaciones antivirus más populares, pero la solución está diseñada únicamente para detectar malware de banca. No se debe utilizar como sustitución de una solución antivirus tradicional.

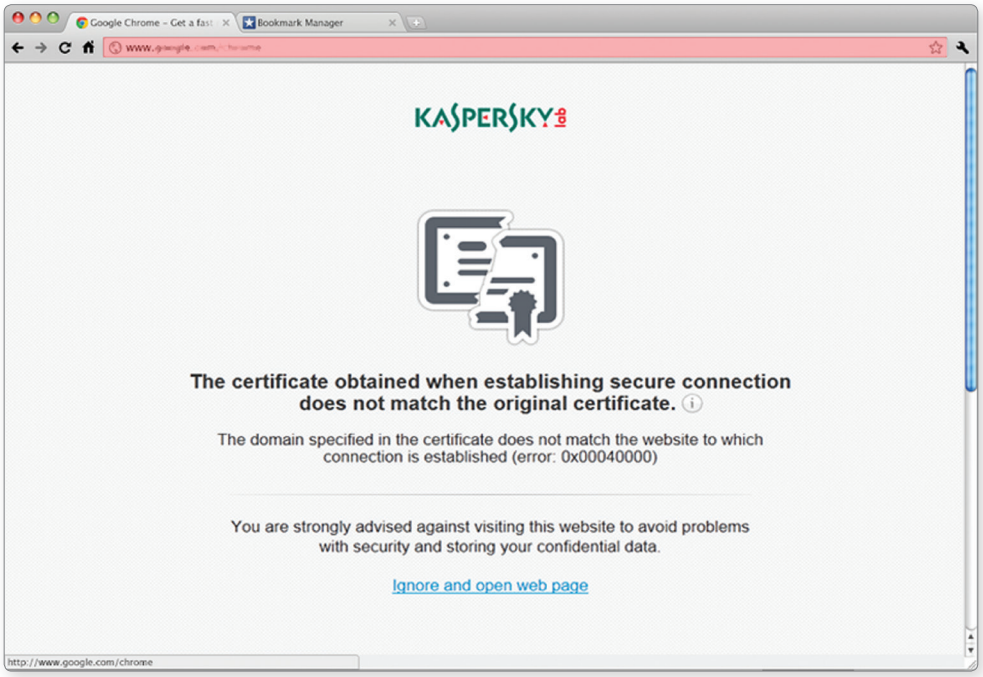
3.3 Protección de las conexiones a Internet

Kaspersky Fraud Prevention no solo garantiza que el ordenador sea un entorno seguro para la banca online y que visite un recurso bancario legítimo. También garantiza que ningún tercero pueda interferir con el canal de Internet entre el banco y sus clientes.

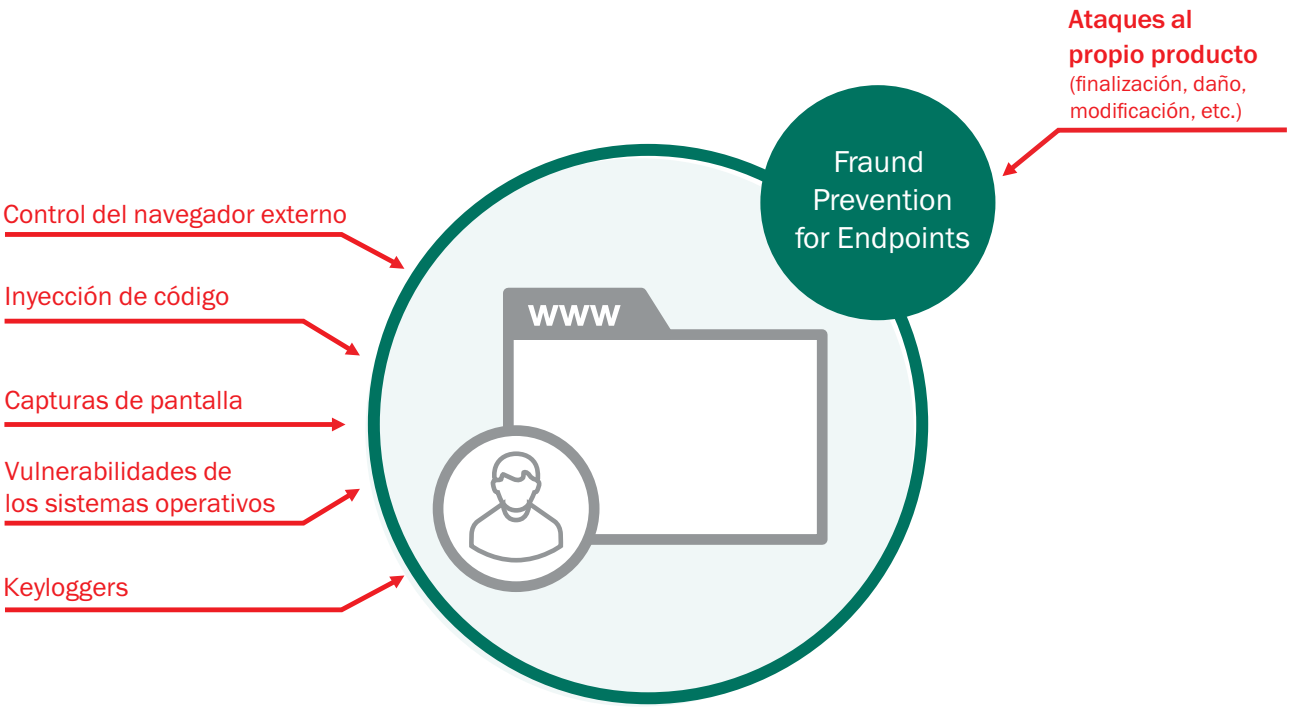
Cada vez que un usuario inicia una sesión de banca online, Kaspersky Fraud Prevention verifica el certificado de seguridad del sitio web comparándolo con el certificado de referencia almacenado en la nube en Kaspersky Security Network. Esta comprobación protege contra ataques del tipo "Man-in-the-Middle" y falsificación de DNS y proxy.



Si se detecta un certificado sospechoso, el sistema alerta al usuario.



3.4 Protección contra amenazas del navegador



3.4.1 Ataques de control del navegador externo

Kaspersky Fraud Prevention for Endpoints ofrece protección de control del navegador con mensajes a las ventanas del navegador (para que terceros no puedan obtener acceso remoto).

3.4.2 Ataques de inserción de código

Protección de la carga de módulos que no son de confianza en el proceso del navegador, verificando la firma DLL localmente y en la nube (KSN).

3.4.3 Protección contra la captura de instantáneas

La protección contra las capturas de pantalla incluye:

- Protección contra las técnicas de captura de pantalla
- Protección de la ventana abierta actualmente en el navegador protegido

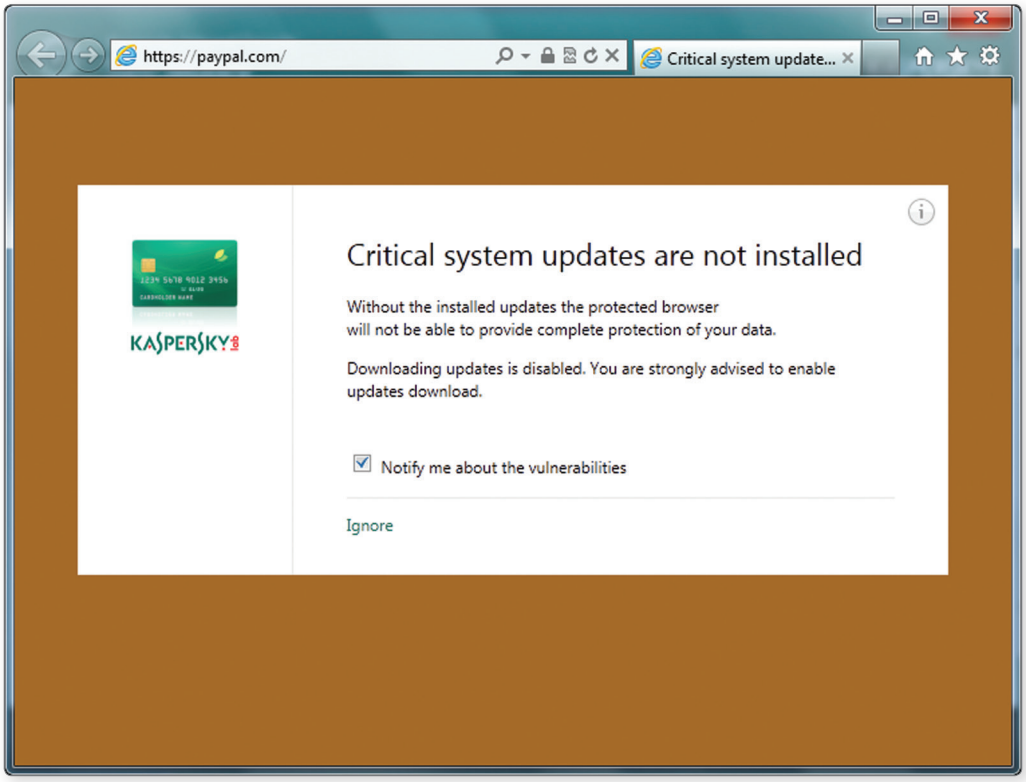
3.4.4 Análisis de vulnerabilidades de los sistemas operativos

Base de datos de vulnerabilidades especializada que se puede actualizar:

- Solo el sistema operativo
- Solo derivación de privilegios del modo de núcleo

3.4.5 Teclado seguro

Cuando se utiliza el navegador protegido, Kaspersky Fraud Prevention for Endpoints protege todos los campos de entrada. Kaspersky Fraud Prevention intercepta y procesa todas las teclas que pulsan a través del controlador del teclado KFP, lo que impide la intercepción de los datos de entrada por malware. Teclado seguro se puede utilizar en Safe Browser y en ventanas del navegador generales.



3.4.6 Protección del portapapeles

Restringe el acceso al portapapeles de las aplicaciones que no sean de confianza.

3.4.7 Autoprotección

Protege contra las modificaciones de Kaspersky Fraud Prevention for Endpoints:

- Claves del registro de Windows
- Archivos
- Procesos
- Subprocesos

4. Consola de gestión de endpoints

La solución Kaspersky Fraud Prevention for Endpoints dispone de una única consola de gestión sencilla que se beneficia de información contextual y correlacionada más exhaustiva y amplia sobre el usuario, el dispositivo del usuario y la sesión.

4.1 Panel de informes

EMC recopila información de Kaspersky Fraud Prevention for Endpoints sobre el dispositivo del usuario, las sesiones y el entorno, así como de todos los ataques lanzados en la máquina del usuario (phishing, ataques mitb o mitm, ataques de malware, etc.)

4.2 Configuración remota de Kaspersky Fraud Prevention for Endpoints

EMC ofrece capacidades de gestión que permiten cambiar la configuración de Kaspersky Fraud Prevention for Endpoints de forma remota.

4.3 Información estadística

EMC incluye un punto de integración que permite el envío de estadísticas a los sistemas de supervisión internos de las transacciones, lo que aumenta el índice de detección y disminuye el número de falsos positivos.

5. Detalles de implementación

La integración consta por lo general de 3 pasos:

1. Personalización de la solución en función de los requisitos del banco para crear un servicio de banca online personalizado. En enfoque de etiquetado blanco de Kaspersky Lab permite que un banco pueda crear su propia experiencia de usuario online utilizando sus propios logotipos, combinaciones de colores, tipos de letra y diseños de página preferidos. Los iconos de escritorio y de la bandeja del sistema también se pueden personalizar exactamente como el banco necesita.
2. Configuración de la integración con los sistemas internos del banco. Kaspersky Fraud Prevention for Endpoints permite la recuperación de los detalles de la versión y el estado del producto al conectarse a un banco online. Esta información se recupera mediante un script especializado, tal como se describe en la documentación. Recomendamos tres escenarios de trabajo principales, pero cada banco es libre de elegir cómo se utilizan los datos recopilados.
3. El banco es libre de elegir la manera de distribuir la aplicación entre sus clientes, por ejemplo, comprobando si Kaspersky Fraud Prevention ya se está ejecutando en los equipos de los usuarios e invitándolos a descargar KASPERSKY FRAUD PREVENTION si es necesario. De forma alternativa, el banco puede elegir otra forma de distribuir la aplicación. Para conservar los recursos informáticos del banco, la mayor parte de la aplicación se almacena en los servidores de Kaspersky Lab, a los que se puede acceder mediante un archivo de descarga de 2 MB que se proporciona al banco durante la fase de implementación.

Normalmente se tarda aproximadamente dos semanas en completar el proceso de instalación. El equipo de implementación especial de Kaspersky Lab está disponible durante todo el proceso de instalación para ayudar a integrar la solución con el resto de la red del banco y resolver cualquier problema que pueda surgir.

Póngase en contacto con nosotros para obtener más información:
Kfp_hq@kaspersky.com
http://www.kaspersky.com/business-security/fraud-prevention

Marzo de 2015/ Global