KASPERSKY FRAUD PREVENTION FOR ENDPOINTS

KASPERSKY lab

www.kaspersky.fr

KASPERSKY FRAUD PREVENTION

1. Techniques d'attaque du système bancaire en ligne

L'appât du gain constitue la principale motivation de la cyber-criminalité. Les gangs criminels sophistiqués de notre époque disposent de tout un arsenal de techniques pour voler de l'argent aux banques et aux services financiers en ligne. Qu'il s'agisse de manipuler des transactions légitimes et de détourner des fonds vers d'autres comptes par le biais de programmes malveillants ou de combiner l'ingénierie sociale et le phishing pour accéder aux comptes, les cyber-criminels utilisent diverses techniques pour voler l'argent des utilisateurs des services bancaires en ligne.

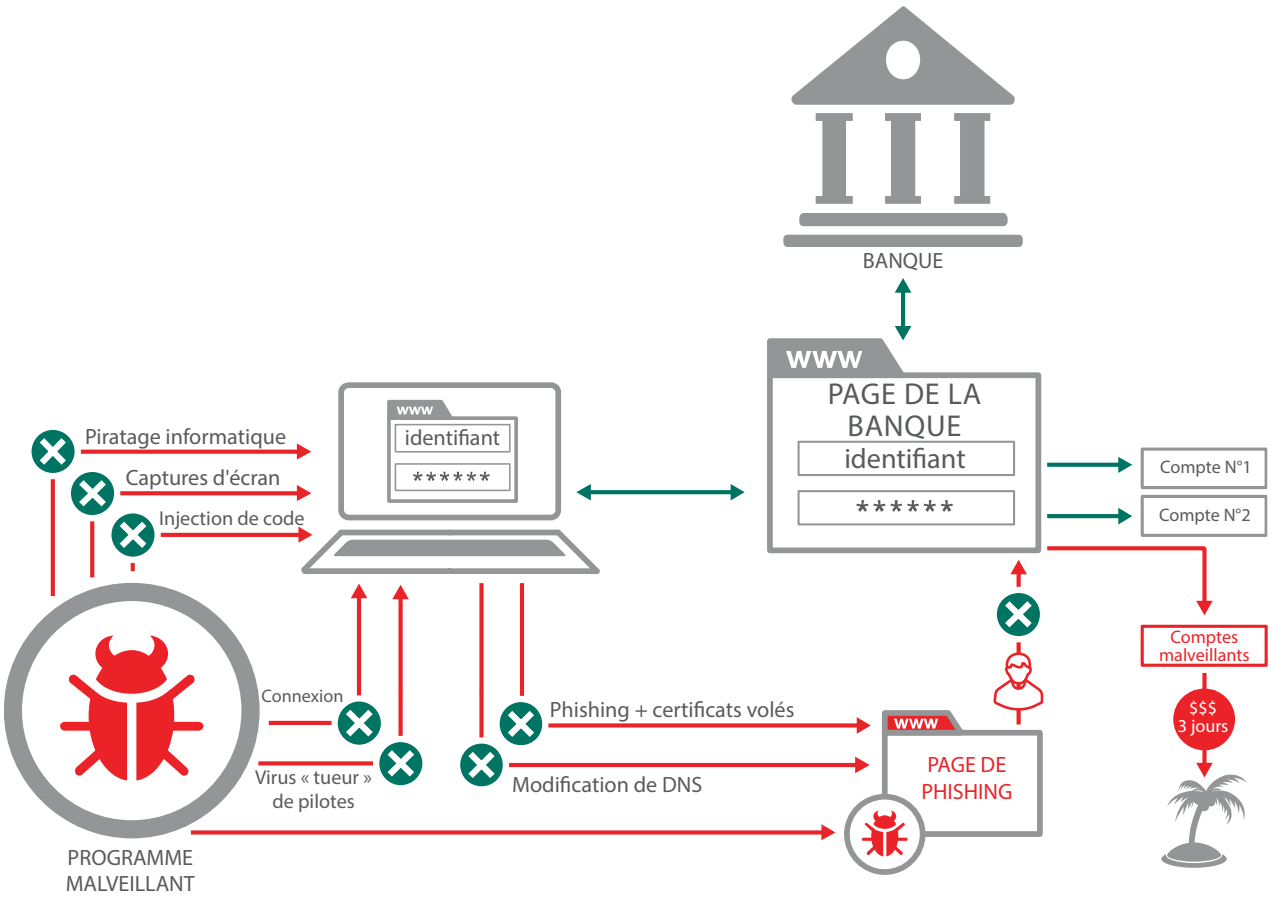
Il existe deux principales menaces :

- Prise de contrôle de compte : voler les données d'identification d'un utilisateur et les utiliser pour voler l'argent sur son compte
- Manipulation de transaction : modifier les données de la transaction ou créer une nouvelle transaction au nom du client

Kaspersky Fraud Prevention for Endpoints vous protège contre les menaces suivantes :

- Vol de données d'identification
  - Phishing
  - Ingénierie sociale
  - Fuite de données
  - Modification de page Web (web-injections)
  - Récupération de formulaire
  - Enregistrement de frappe
  - Capture d'écran
  - Attaques de spoofing*
- Manipulation de transaction
  - Attaque dite de l'homme du milieu*
  - Accès à distance
  - Attaque dite de l'homme dans le navigateur*

2. Prévention de la fraude



1 Le spoofing en finance est une technique de manipulation boursière qui consiste à offrir des titres à la vente ou l'achat dans l'intention d'annuler l'ordre juste avant qu'il soit exécuté, et ceci afin d'obtenir un mouvement favorable des prix.
2 L'attaque dite de l'homme du milieu est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.
3 L'attaque dite de l'homme dans le navigateur s'attaque aux navigateurs pour modifier les pages Internet, modifier le contenu des transactions ou en ajouter de nouvelles

3. Technologies de protection

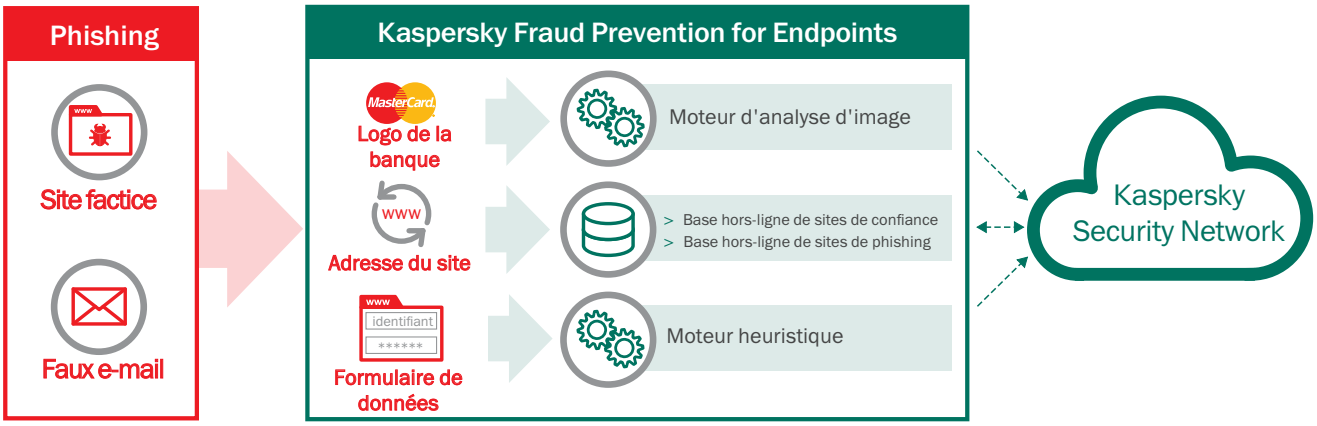
3.1 Protection contre le phishing

Le système de protection contre le phishing de Kaspersky Lab combine des technologies heuristiques et dans le cloud à des bases de données hors ligne traditionnelles pour bloquer les menaces, même en cours d'apparition ou encore indétectables.

Le module Cloud Anti-Phishing (lutte contre le phishing dans le cloud), qui est rapidement mis à jour, contient des masques d'URL de phishing. Les nouvelles menaces peuvent être ajoutées quelques secondes après leur détection, ce qui protège vos ordinateurs contre les sites de phishing qui ne figurent pas encore dans les bases de données locales. Quand un utilisateur rencontre une URL ne figurant pas dans la base de données locale, le système effectue automatiquement une vérification dans le cloud.

L'élément Web du système de protection contre le phishing est déclenché quand l'utilisateur clique sur un lien vers une page de phishing ne figurant pas encore dans les bases de données de Kaspersky Lab.

En outre, une vaste base de données hors ligne de lutte contre le phishing, qui est enregistrée sur les appareils de l'utilisateur, contient tous les masques les plus courants d'URL de phishing.



3.2 Analyse et suppression des programmes malveillants

Même quand un programme malveillant s'est déjà logé sur l'ordinateur d'un utilisateur, Kaspersky Fraud Prevention peut protéger les opérations bancaires en ligne. Dès qu'il est installé, Kaspersky Fraud Prevention réalise une analyse du système pour détecter les programmes malveillants ciblant les opérations bancaires. Les utilisateurs sont informés de tout problème et sont invités à supprimer les fichiers malveillants pour désinfecter leur ordinateur. La solution lance une analyse supplémentaire chaque fois que le navigateur bancaire protégé est démarré.

ÉTUDE DE CAS

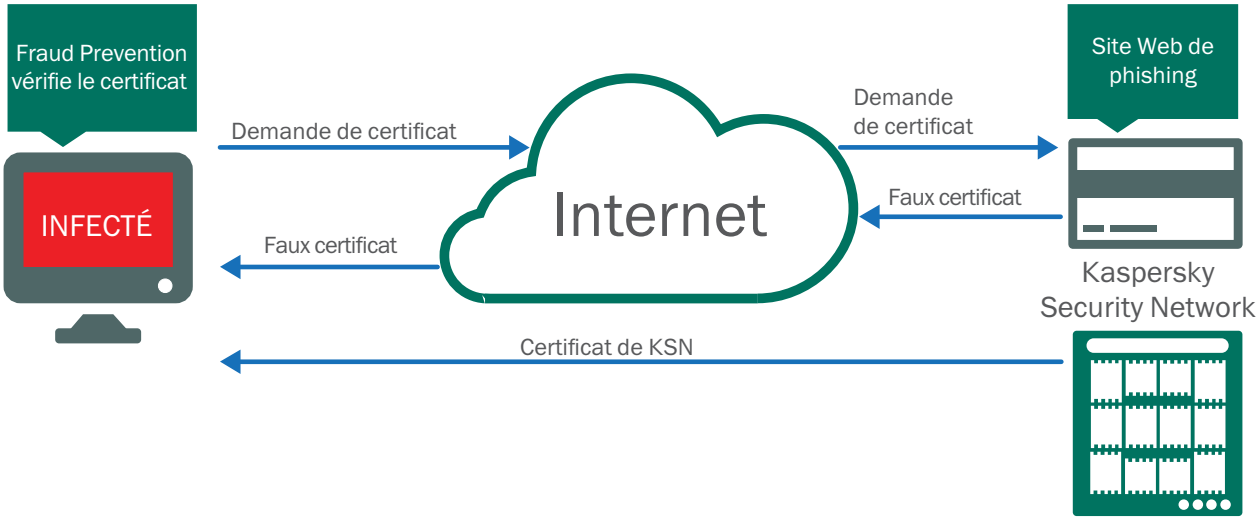
Une grande banque russe est devenue la cible d'un programme malveillant redirigeant automatiquement les clients vers une page de phishing. Cette astuce a poussé les utilisateurs à communiquer directement leurs données d'identification bancaire aux cybercriminels et a bloqué l'accès au site Web réel de la banque par la suite. Kaspersky Fraud Prevention a pu supprimer les programmes malveillants sur les ordinateurs des clients pour leur permettre de réaliser des opérations bancaires en toute sécurité.

Kaspersky Fraud Prevention for Endpoints est compatible avec la plupart des applications antivirus les plus populaires, mais cette solution a été uniquement conçue pour identifier les programmes malveillants ciblant les opérations bancaires. Il ne convient pas de l'utiliser à la place d'une solution antivirus traditionnelle.

3.3 Protection des connexions Internet

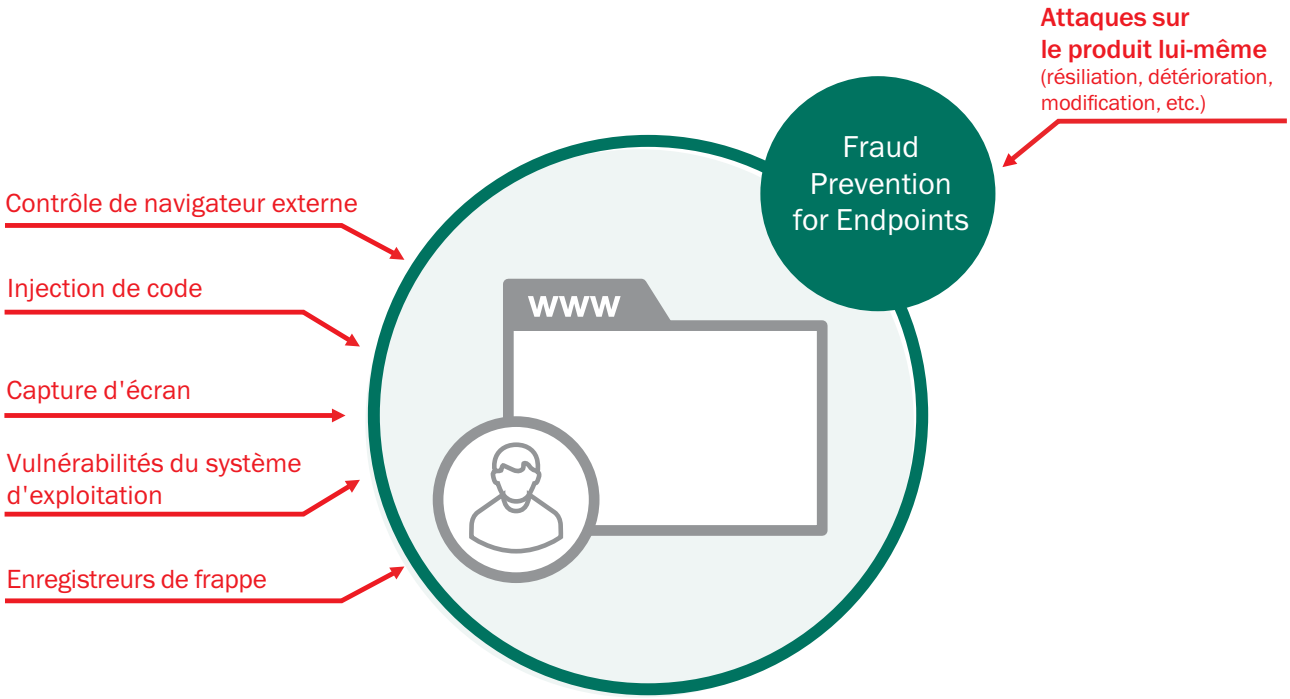
Kaspersky Fraud Prevention ne se contente pas de veiller à la sécurité de l'environnement informatique pour réaliser des opérations bancaires ou de vérifier qu'une ressource bancaire visitée est légitime. Il s'assure également qu'aucun tiers n'est en mesure de nuire à la voie de communication Internet reliant la banque à ses clients.

Chaque fois qu'un utilisateur ouvre une session bancaire en ligne, Kaspersky Fraud Prevention vérifie le certificat de sécurité du site Web en comparant le certificat de référence enregistré en ligne dans Kaspersky Security Network. Ce contrôle vous protège contre les attaques dite de l'homme du milieu, ainsi que contre le spoofing de DNS et de proxy.



Si le système détecte un certificat suspect, il alerte l'utilisateur.

3.4 Protection contre les menaces dans le navigateur



3.4.1 Attaques de contrôle de navigateur externes

Kaspersky Fraud Prevention for Endpoints assure votre protection contre le contrôle de navigateur en envoyant des messages dans les fenêtres du navigateur (pour qu'aucun tiers ne puisse obtenir un accès à distance).

3.4.2 Attaques par injection de code

Protection contre le chargement de modules non fiables dans le processus du navigateur, vérification de la signature DLL localement et dans le cloud (KSN).

3.4.3 Protection contre les captures d'écran

La protection contre les captures d'écran comprend :

- Protection contre les techniques de capture d'écran
- Protection de la fenêtre ouverte dans le navigateur protégé

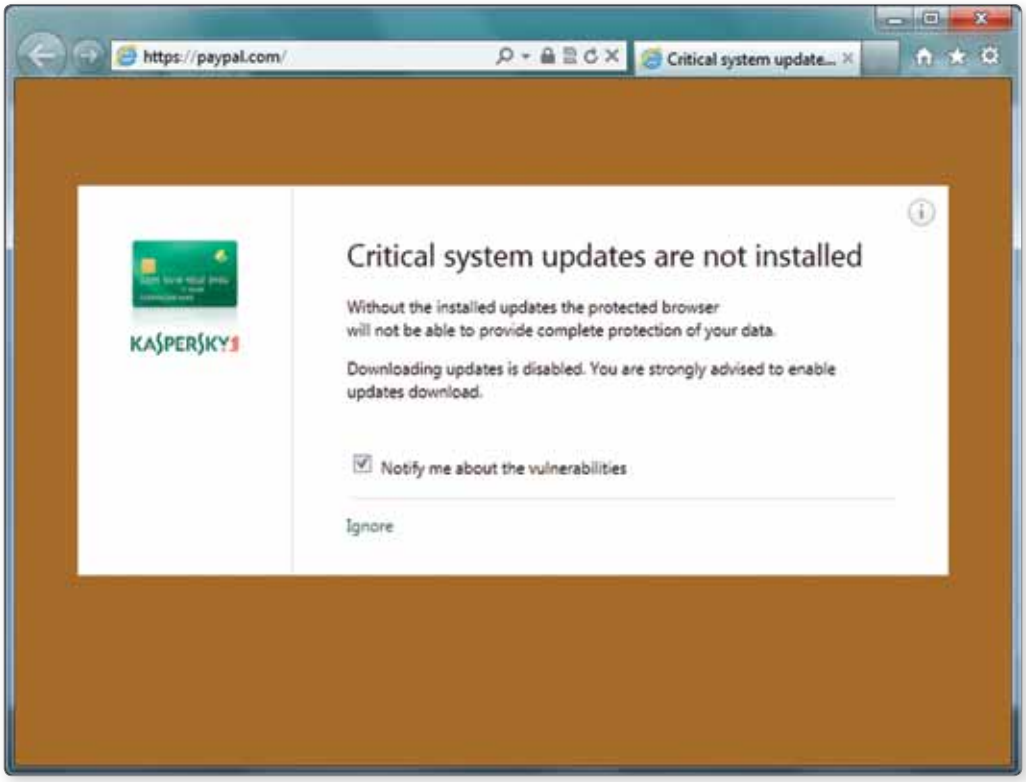
3.4.4 Analyse des vulnérabilités du système d'exploitation

Base de données pouvant être mise à jour et dédiée aux vulnérabilités :

- Système d'exploitation seulement
- Transmission des problèmes seulement avec les privilèges du mode Kernel

3.4.5 Protection de clavier

Quand un navigateur protégé est utilisé, Kaspersky Fraud Prevention for Endpoints sécurise toutes les saisies. Kaspersky Fraud Prevention capture et traite toutes les frappes de clavier par le biais du pilote de clavier KFP, ce qui évite la capture de la saisie de données par des programmes malveillants. Le clavier sécurisé peut être utilisé dans Safe Browser dans les fenêtres de navigation ordinaires.



3.4.6 Protection du presse-papiers

Limite l'accès des applications non fiables au presse-papiers.

3.4.7 Auto-protection

Protection contre les modifications de Kaspersky Fraud Prevention for Endpoints :

- Clés de registre Windows
- Fichiers
- Processus
- Fils

4. Console de gestion de terminal

La solution Kaspersky Fraud Prevention for Endpoints propose une console unique pour faciliter la gestion avec des informations contextuelles et connexes plus poussées et plus globales concernant l'utilisateur, l'appareil de l'utilisateur et la session.

4.1 Tableau de bord de communication

EMC recueille des informations auprès de Kaspersky Fraud Prevention for Endpoints concernant l'appareil de l'utilisateur, les sessions et l'environnement, ainsi que sur les attaques lancées contre le système de l'utilisateur (phishing, attaques mitb ou mitm, programmes malveillants).

4.2 Configuration à distance de Kaspersky Fraud Prevention for Endpoints

EMC fournit des fonctions de gestion permettant de modifier les paramètres de Kaspersky Fraud Prevention for Endpoints à distance.

4.3 Flux statistique

EMC dispose d'un point d'intégration pour envoyer des statistiques à des systèmes internes de surveillance des transactions, ce qui augmente le taux de détection tout en réduisant le nombre de faux positifs.

5. Informations de mise en œuvre

L'intégration se compose généralement de 3 étapes :

1. Personnalisation de la solution en fonction des besoins de la banque pour créer un service bancaire en ligne sur mesure. L'approche de marque blanche adoptée par Kaspersky Lab permet à la banque de créer sa propre expérience d'utilisateur en ligne et d'utiliser ses propres logos, couleurs, caractères et mises en page. Il est également possible de personnaliser les icônes de bureau et de barre d'état selon les souhaits de la banque.
2. Configuration de l'intégration avec les systèmes internes de la banque. Kaspersky Fraud Prevention for Endpoints permet de récupérer les informations sur la version du produit et son statut lors de la connexion à une banque en ligne. Ces informations sont extraites par un script dédié, comme indiqué dans la documentation. Nous recommandons trois principaux scénarios de travail, bien que chaque banque ait la possibilité de choisir la façon dont elle utilisera les données récupérées.
3. La banque peut alors décider du mode de distribution de l'application parmi ses clients, par exemple en vérifiant si Kaspersky Fraud Prevention est déjà installé sur les ordinateurs des clients et en les invitant à télécharger KASPERSKY FRAUD PREVENTION le cas échéant. La banque peut aussi choisir une autre façon de distribuer l'application. Pour conserver les ressources informatiques de la banque, la plus grande partie de l'application est stockée sur les serveurs de Kaspersky Lab et l'accès est possible grâce à un fichier de téléchargement de 2 Mo remis à la banque pendant la phase de mise en œuvre.

Le processus d'installation prend généralement deux semaines. L'équipe de mise en œuvre spéciale de Kaspersky Lab est disponible tout au long de la phase d'installation pour faciliter l'intégration de la solution au réseau de la banque et pour résoudre tout problème éventuel.

Pour en savoir plus, contactez-nous sur : kfp@kaspersky.fr
http://www.kaspersky.fr/business-security/fraud-prevention

Mars15/ Global