KASPERSKY FRAUD PREVENTION - CLIENTLESS ENGINE

Une sécurité plus intelligente - des services bancaires en ligne plus performants

Alors que les institutions financières se battent pour offrir aux clients l'expérience de services bancaires en ligne la plus intuitive et la plus satisfaisante, les cybercriminels professionnels se battent pour développer des programmes malveillants encore plus sophistiqués pour profiter pleinement de chaque nouvelle possibilité de fraude en ligne.

Exemples de nouvelles techniques d'attaque puissantes en cours que vous pouvez déjà avoir rencontrées :

- **Infiltration de page Web** : champs supplémentaires « injectés » sur votre page de connexion, capturant des données de clients confidentielles, telles que le numéro de carte CVS pour une utilisation dans des attaques par « carte non présente ».
- **Fausses fenêtres pop-up (phishing)** : ajout d'une fenêtre « pop-up » du pirate demandant des données supplémentaires, peut-être un numéro de téléphone portable, pour intercepter des vérifications à 2 facteurs.
- **Altération de transaction** : il s'agit par exemple de donner l'ordre aux clients de « repayer » de l'argent faussement enregistré lorsqu'ils entrent sur leur compte par erreur, ou de faire une transaction « test » afin d'aider la banque.

Toutes ces techniques commencent par le chargement de programmes malveillants, généralement sous la forme de chevaux de Troie bancaires, sur votre système bancaire en ligne. Ce programme malveillant est introduit par le point le plus vulnérable de votre système : vos clients. Les pirates commencent par infecter l'appareil de votre client, puis utilisent la connexion en ligne du client à votre site comme point d'entrée.

Comment vous protégez-vous contre les attaques frauduleuses complexes initiées à partir d'appareils d'utilisateurs infectés, sans compromettre l'expérience bancaire en ligne intuitive et simple qui rend les clients heureux et fidèles ?

Kaspersky Fraud Prevention Clientless Engine empêche les cybercriminels de lancer des attaques réussies par :

La détection des programmes malveillants financiers :
Recherche et identification proactives des programmes malveillants tentant d'infecter vos pages Web par les appareils de vos clients.

Détection de tout ordinateur ou téléphone mobile infecté tentant de lancer des activités malveillantes à travers sa connexion en ligne à votre site, sans aucun impact sur les clients non infectés ou leur expérience bancaire numérique.

La génération de rapports complets :
Alertes permettant à votre banque de prendre les mesures suivantes :

- Blocage de la transaction
- Fermeture de la session de l'utilisateur
- Gestion du cas du client pour s'assurer que l'incident ne se répète pas.

La gestion des terminaux :
Fourniture de données d'incident grâce à la console d'administration de Kaspersky Fraud Prevention et transfert à des systèmes internes ou tiers pour des analyses et des recherches complémentaires, si nécessaire.

Des flux d'informations :
Fourniture à vos équipes de gestion bancaire en ligne des informations dont elles ont besoin pour prendre des décisions de sécurité complexes.

Tandis que vous avez la visibilité de chaque incident potentiel, le processus n'implique aucune inquiétude pour les utilisateurs, à moins que leur appareil n'ait été compromis par des programmes malveillants bancaires. Dans ce cas, vous serez là pour les rassurer et les conseiller sur la façon de rester en sécurité à l'avenir.

Vous créez ainsi un environnement bancaire en ligne plus sûr pour tout le monde, vous permettant de conquérir et de fidéliser davantage de clients, en développant davantage les fonctionnalités de votre portail bancaire numérique, sans accroître le risque de tentatives de fraude non détectées.

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

Fiche d'information sur Kaspersky Fraud Prevention Clientless Engine, Août 2015 GL