feedzai

Bloquez les RAT et les logiciels malveillants avant qu'ils ne nuisent à vos clients

Plus d'un milliard de clients à travers le monde nous font confiance pour éviter chaque année plus d'un milliard de dollars de pertes

مصرف الراجحي alrajhi bank · jack henry · stet · zeller

La fraude bancaire sur mobile et en ligne est de plus en plus le fait de logiciels malveillants et de chevaux de Troie d'accès à distance (Remote Access Trojans, RAT). Les RAT ont souvent recours à l'ingénierie sociale : les victimes sont amenées, par le biais d'appels frauduleux, à télécharger des outils d'accès à distance légitimes, tels que TeamViewer ou AnyDesk. Une fois l'accès à l'appareil obtenu, les fraudeurs peuvent récupérer des identifiants, détourner des sessions bancaires actives en temps réel et effectuer des paiements à l'insu de l'utilisateur, le tout sans que la banque ne se rende compte que la session n'est pas légitime.

À mesure que l'utilisation des appareils mobiles se généralise, les menaces liées aux RAT et aux logiciels malveillants évoluent, ciblant à la fois les vulnérabilités connues et les attaques « zero-day ». La protection contre ces menaces devient également une nécessité réglementaire, des cadres tels que la directive PSD2/SCA exigeant des mesures de protection contre les logiciels malveillants pouvant être démontrées.

Pour mettre en place une défense de premier ordre, les institutions doivent adopter une approche intégrée, en exploitant les informations sur les menaces provenant des appareils en synergie avec les processus décisionnels liés aux transactions. Cette approche permet d'identifier les risques plus tôt dans le parcours client et de mettre en place des mesures de prévention adaptées à la stratégie de gestion des risques de chaque banque.



L’approche globale de Feedzai pour détecter et protéger contre les logiciels malveillants et les attaques de type RAT

En associant les informations issues des appareils et du réseau, la biométrie comportementale, les signaux liés aux comptes et les données de paiement, les organisations peuvent détecter plus tôt et avec une plus grande précision les risques liés aux logiciels malveillants et aux RAT.

Connexion	Activité en cours	Sortant	Connexion	Activité en cours	Activité en cours	Sortant
Connexion de la victime	**Mise à jour du compte**	**Paiement initié**	**Connexion du fraudeur**	**Détection d’un RAT**	**Création du bénéficiaire**	**Paiement initié**
Appareil et comportement habituels	Le numéro de téléphone associé au compte a été modifié	Paiement régulier initié	Appareil habituel	Le RAT a établi une session à distance ou une manipulation de type « man-in-the-browser » via l’appareil habituel du client	Un nouveau bénéficiaire est créé au cours de la même session	Un paiement important suit immédiatement
				Point d’élimination potentiel		**Point d’élimination potentiel**

Principaux avantages de l’approche Feedzai

Détection des menaces connues et des attaques « zero-day »
Tirez parti de SDK mobiles et JavaScript avancés pour identifier la cause première des menaces, en détectant en temps réel les familles de logiciels malveillants connues et les vulnérabilités « zero-day » émergentes. Les signaux actuels et historiques sont analysés afin de mettre en évidence, avec une grande précision, l’évolution des schémas de menaces.

Assurer la sécurité tout au long du parcours client
Détectez les appareils compromis lors de la mise en service en analysant les applications installées et en signalant les logiciels malveillants, les applications suspectes et les anomalies au niveau des privilèges avant la création du compte. Assurez une protection continue lors de la connexion et au cours des activités quotidiennes en surveillant les signaux liés aux comportements, aux appareils et au réseau afin de détecter les prises de contrôle à distance, les logiciels malveillants et les menaces « zero-day ».

Faire confiance à chaque décision
Tirez parti des défenses multicouches qui associent les indicateurs de RAT et de logiciels malveillants à des modèles transactionnels. Ces indicateurs comprennent la détection des logiciels malveillants, les sessions à distance, les appareils inhabituels, la biométrie comportementale, la détection d’applications et les changements de bénéficiaires. Cette approche de premier ordre analyse les comportements observés après une intrusion afin d’améliorer la détection des prises de contrôle de comptes (Account Takeover, ATO), des escroqueries et des activités de « mule », tout en limitant le nombre de faux positifs.

Une protection immédiate et en constante évolution
Accélérez le retour sur investissement grâce à des stratégies préconfigurées permettant de bloquer les RAT et la fraude liée aux logiciels malveillants. Utilisez des ensembles de règles et des modèles d'apprentissage automatique pour détecter les attaques de type « man-in-the-browser » et les détournements de session à partir de signaux comportementaux et liés aux appareils. Feedzai réentraîne en permanence ses modèles à l'aide de données confirmées relatives à la fraude afin d'améliorer la détection au fil du temps.

Intervenir au bon moment
Agissez rapidement dès qu'une menace est confirmée grâce à des capacités d'intervention flexibles, allant du masquage des écrans lors de la détection d'une session à distance à la coupure forcée des sessions compromises avant que des pertes ne surviennent. Les règles combinant les paiements et la détection des logiciels malveillants vous permettent de déclencher des réponses immédiates lors de la connexion, lors d'une modification de compte ou au niveau du paiement.



Exemple de réussite

Une grande banque européenne protège plus de 15 millions de clients contre la fraude liée aux logiciels malveillants

Problème
Une grande banque européenne comptant plus de 15 millions de clients a dû faire face à une pression croissante due à des attaques sophistiquées menées à l'aide de logiciels malveillants et de RAT. Elle avait besoin d'une solution permettant de protéger ses utilisateurs contre toute manipulation, d'empêcher le vol d'identifiants et de garantir le strict respect des réglementations régionales.

Solution
La banque a établi des profils de référence relatifs au comportement des clients à l'aide de modèles d'intelligence artificielle permettant d'analyser les données biométriques, celles relatives aux appareils et celles du réseau, ce qui lui a permis de détecter les identifiants volés et les attaques par accès à distance. Elle a ensuite mis en place des mécanismes de réponse automatisée afin d'intervenir et d'empêcher que les utilisateurs ne soient manipulés en vue de compromettre leurs sessions.

Résultats

Réduction des pertes liées à la fraude sans nuire à l'expérience client

Optimisation des opérations de lutte contre la fraude et des coûts liés aux centres d'appels

Conformité assurée aux réglementations SCA/PSD2 et en matière de lutte contre le blanchiment d'argent

Les solutions unifiées de Feedzai pour protéger les clients contre les RAT et les logiciels malveillants

Confiance numérique
Assurez en toute discrétion la protection de l'ensemble du parcours client, de l'intégration à la connexion, en passant par les activités courantes des clients, grâce à une protection basée sur un SDK et JavaScript. Associez la biométrie comportementale, les informations issues des appareils et les informations issues du réseau pour détecter en temps réel les RAT, les logiciels malveillants et les sessions compromises. Mettez en œuvre des mesures de prévention immédiates pour bloquer automatiquement les activités malveillantes ou mettre fin aux sessions à haut risque, ce qui permet une intervention ciblée tout en minimisant les perturbations pour les clients légitimes.

Fraude aux transactions dans le secteur bancaire
Reçoit en temps réel des alertes concernant les logiciels malveillants et les RAT directement de Digital Trust, qui sont utilisées pour améliorer les décisions relatives aux transactions. Des règles prêtes à l'emploi, applicables à l'ensemble des flux de travail liés aux transactions et aux activités numériques, réagissent aux indicateurs RAT en les combinant avec des profils comportementaux, des scores de risque de session, l'historique des bénéficiaires et le contexte des transactions. Par conséquent, si une transaction est signalée par un indicateur RAT actif, elle peut être immédiatement refusée ou transmise, avec un score de risque élevé, à un analyste pour examen. Il en résulte une intervention précise et sûre qui permet d'éviter toute perte de fonds.

Reconnu par IDC datos INSIGHTS Celent. Chartis

Bloquez les RAT et les logiciels malveillants en temps réel

Demander une démo

sales@feedzai.com
info@feedzai.com
feedzai.com

