LexisNexis®
RISK SOLUTIONS

ÉTUDE DE CAS

LexisNexis® Risk Solutions aide un grand établissement financier à réduire les attaques de logiciels malveillants et les pertes liées à la fraude

Les renseignements sur l'identité numérique fournis par la solution LexisNexis® ThreatMetrix® détectent les événements à haut risque en temps quasi réel, sans nuire à l'expérience utilisateur

EN BREF

ENTREPRISE

Grand établissement financier

CAHIER DES CHARGES

- Prévenir les attaques d'ingénierie sociale ciblées qui infiltrent les comptes d'utilisateurs de confiance à l'aide de logiciels d'accès à distance.
- Endiguer les attaques de logiciels malveillants.
- Limiter les événements frauduleux lors de la connexion et du paiement.
- Réduire les pertes liées à la fraude.

SOLUTION

LexisNexis Risk Solutions a mis en place une solution complète de profilage comportemental, en temps quasi réel, d'un bout à l'autre des sessions en ligne. Couvrant la création de compte, la connexion, la modification des détails et des préférences, la navigation dans le compte, la création de nouveaux bénéficiaires et le profilage des paiements, elle permet de repérer les anomalies indiquant la présence d'un logiciel malveillant ou d'un utilisateur illégitime de logiciel d'accès à distance. Cette initiative a considérablement réduit le taux de fraude, tout en assurant aux clients de confiance une expérience sans points de friction.

RÉSULTAT

- Neutralisation très rapide des attaques ciblées de logiciels malveillants, sans aucun faux positif.
- Détection et blocage des tentatives d'usurpation d'identité.
- Détection des attaques de type « Man-In-The-Browser » visant à duper les utilisateurs afin de les amener à divulguer des informations d'identité.
- Détection des logiciels d'accès à distance utilisés de manière illégale pour l'usurpation de comptes.
- Plusieurs millions de dollars d'économies mensuelles réalisées en matière de fraude.

Présentation

Cet établissement financier offre un large éventail de prestations, parmi lesquelles des services bancaires aux particuliers et aux entreprises, des services d'assurance, des services financiers aux entreprises et des services bancaires privés. Sa philosophie : répondre efficacement aux besoins des clients et fournir une gamme complète de services d'exception. Protéger les clients contre la fraude tout en leur assurant une expérience en ligne sans points de friction constitue un impératif clé.

Avec LexisNexis Risk Solutions, cet établissement financier peut :

- Identifier les événements liés à des appareils qui utilisent des outils d'antidétection pour contourner la prise d'empreintes numériques des terminaux en changeant de version de navigateur, de plug-ins installés dans le navigateur, de type de système d'exploitation, de fuseau horaire, etc.
- Reconnaître la présence de logiciels malveillants en analysant les modèles comportementaux ou la modification des pages Web, en rejetant les événements frauduleux et en signalant ceux qui paraissent suspects.
- Détecter les chevaux de Troie d'accès à distance (RAT, Remote Access Trojan) qui tentent de voler des informations personnelles ou de pirater la session de connexion légitime d'un utilisateur.

Enjeu Commercial

Comme beaucoup d'autres, cet établissement financier faisait face à un nombre croissant d'attaques d'ingénierie sociale bien orchestrées qui conduisaient souvent les utilisateurs à installer malgré eux des logiciels d'accès à distance ou des logiciels malveillants. Ces attaques parvenaient parfois à franchir des barrières d'authentification forte à deux facteurs, par exemple en piratant des sessions de connexion parfaitement authentifiées.

Lorsque des clients accédaient au site Web pour se connecter à leur compte bancaire, effectuer un paiement, modifier leur mot de passe, etc., ces logiciels malveillants surveillaient les clics sur les boutons, ainsi que les champs contenant des données personnelles, notamment le nom du client, le numéro de compte, les mots de passe et autres informations confidentielles.

Cet établissement financier avait besoin d'une solution performante de protection contre la fraude, capable d'analyser les données relatives aux événements actuels et de les comparer aux comportements historiques afin d'identifier clairement les comportements anormaux en temps quasi réel. Les événements témoignant d'un comportement anormal pourraient ensuite être signalés pour examen ou être directement rejetés en fonction du risque associé.

ÉTUDE DE CAS

Cet établissement financier avait besoin d'une solution performante de protection contre la fraude, capable d'analyser les données relatives aux événements actuels et de les comparer aux comportements historiques afin d'identifier clairement les comportements anormaux en temps quasi réel.

Exploitation de la puissance des renseignements partagés à l'échelle mondiale pour une détection des événements à haut risque en temps quasi réel

La meilleure façon de lutter contre le problème complexe du cybercrime organisé est d'exploiter la puissance d'un réseau mondial partagé. Le réseau d'identités numériques Digital Identity Network® de LexisNexis® collecte et traite les renseignements partagés à l'échelle mondiale provenant de millions d'interactions client quotidiennes, dont les connexions, les paiements et les demandes de nouveau compte. En tirant parti des capacités de la solution LexisNexis® ThreatMetrix® et en s'appuyant sur les informations fournies par le réseau d'identités numériques Digital Identity Network, LexisNexis® Risk Solutions crée une identité numérique unique pour chaque utilisateur en analysant les innombrables liens entre les appareils, les lieux et les informations personnelles anonymisées. Les comportements qui s'écartent de cette identité numérique de confiance sont détectés avec précision et en temps quasi réel, alertant l'établissement financier d'une possible tentative de fraude. Les comportements suspects sont identifiés et signalés pour vérification, authentification renforcée ou rejet avant le traitement de la transaction, ce qui assure une expérience fluide aux utilisateurs de confiance.

La solution ThreatMetrix a pu :

- Identifier les comportements et associations de confiance pour chaque utilisateur (appareils, adresses IP, lieux, comportement de session et habitudes de paiement).
- Identifier les changements de comportement anormaux pour prévenir la fraude aux paiements, notamment en détectant la présence de signatures comportementales de logiciels d'accès à distance et de logiciels malveillants.
- Identifier la présence de réseaux de fraude persistants par corrélation croisée avec des renseignements sur les comptes de mules connus ou avec des comportements frauduleux observés ailleurs dans le réseau LexisNexis Risk Solutions.
- Identifier les anomalies comportementales liées à la fraude d'initiés.

ÉTUDE DE CAS

Principales fonctionnalités de la solution LexisNexis® ThreatMetrix®

- **La technologie de prise d'empreintes numériques des pages** Web protège les transactions en ligne grâce à la détection en temps quasi réel de toute modification des pages, comme l'injection de composants HTML ou JavaScript par des logiciels malveillants.
- **La protection contre les logiciels malveillants** aide les entreprises à atténuer les risques d'attaque de logiciels malveillants, même les plus sophistiqués, réduisant ainsi la fraude. Cela inclut les attaques « Man-In-The-Browser » (MITB), les chevaux de Troie d'accès à distance (RAT), les attaques haute vitesse/fréquence perpétrées par des bots, les attaques lentes et de faible intensité imitant le comportement de clients légitimes, les rançongiciels, les tentatives d'enregistrement de frappe, etc.
- **Les fonctions de détection des logiciels malveillants et de réputation des applications,** incluses dans le SDK (Software Development Kit) mobile, évaluent toutes les applications installées sur les appareils fonctionnant sous Android et les vérifient par rapport à une base de données de signatures unique répertoriant plus de 15 millions d'applications mobiles. Les applications de confiance connues sont validées, tandis que celles qui contiennent des logiciels malveillants ou souffrent d'une mauvaise réputation sont signalées en temps quasi réel.
- **La technologie Honeypot** (« pot de miel » en anglais) pose des leurres afin de détecter les modifications non autorisées apportées aux pages Web dans le navigateur. Le but du « pot de miel » est de se faire passer pour un utilisateur qui naviguerait vers le type de site Web de grande valeur généralement ciblé par les logiciels malveillants. Lorsque le logiciel malveillant tente de s'y attaquer, en injectant du contenu Web supplémentaire, tel que des éléments de formulaire ou des boîtes de dialogue contextuelles nécessitant la saisie d'informations personnelles, notre pot de miel repère ces changements en temps quasi réel.
- **LexisNexis® Risk Solutions peut gagner en performances** en englobant des flux de renseignements externes sur les menaces via une plate-forme d'intégration. Cette plate-forme permet aux établissements d'intégrer des sources de données tierces pertinentes et des prestations personnalisées pour offrir des services d'authentification et de vérification de l'identité supplémentaires dans le cadre des transactions à risque.

LexisNexis® RISK SOLUTIONS

Pour plus d'informations, appelez le 866.528.0780
ou rendez-vous sur risk.lexisnexis.com/FIM-EN