Pindrop : l'empreinte vocale au nom de la lutte anti-fraude téléphonique

En 2016, la **fraude téléphonique** a représenté une perte de 14 milliards de dollars aux Etats-Unis. Par fraude, il faut entendre la récupération de données personnelles auprès des centres d'appels par des malfaisants qui exploitent ces informations à travers des opérations mercantiles.

Par exemple, obtenir d'un support téléphonique la réinitialisation du mot de passe d'un compte bancaire en ligne afin de le pirater.

C'est pour lutter contre ce type de fraude téléphonique qu'est né **Pindrop** en 2011 à Atlanta (Georgie, USA).

Depuis sa création par un trio de fondateurs (Paul Judge, Dr. Mustaque Ahamad, Vijay Balasubramaniyan toujours CEO), la société technologique a levé120 millions de dollars, dont 75 millions obtenus en janvier 2016 via le fonds corporate Google Capital. L'effectif se porte à 310 salariés aujourd'hui.

« L'outil téléphonique est très utilisé par les entreprises comme vecteur d'activités économiques mais il n'est pas sécurisé au même niveau que l'informatique », souligne Vincent Pajot, Directeur des ventes Europe du sud de Pindrop.

« Les fraudeurs, qui s'organisent comme de vrais industriels, sont au fait des méthodologies des call centers. Neuf fois sur dix, ils connaissent l'ensemble des réponses aux questions d'authentification. Un fraudeur passe entre 3 et 5 appels pour faire de 'l'ingénierie sociale' avant d'arriver à ses fins. »

Cette technique d'arnaque qui s'appuie sur la manipulation par téléphone ou par mail des collaborateurs d'une entreprise.

« On constate une explosion des tentatives de fraudes », évoque Vincent Pajot. « *En Europe, en 2015 , 1 appel sur 2□500 était frauduleux. Il est de 1 pour 700 appels aujourd'hui. Un taux qui, chez certains clients que je ne peux pas citer, monte à 1 pour 100. »*

1300 critères vérifiés

Pindrop développe des solutions de détection de fraudes au travers du canal téléphonique à partir de trois technologies principalement.

Pindrop Network permet de vérifier la validité du numéro appelant, à savoir qu'il est bien attribué par un opérateur et n'a pas été usurpé.

Ensuite, **Phone Printing** analyse le contexte audiophonique.*« On identifie l'appareil utilisé pour l'appel et vérifie la correspondance entre cet appareil et le numéro, par exemple qu'un portable n'utilise pas un numéro de ligne fixe »*, explique Vincent Pajot.

Le « bruit de confort » [qui pallie les blancs dans les conversations donnant l'impression que la

communication est coupée, NDLR] – spécifique à chaque téléphone, tout comme son micro – est également analysé.

« On regarde tout ça, ainsi que la géolocalisation au niveau du pays via les particularités des réseaux empruntés. »

Au total, 1300 critères biométriques analysés en une vingtaine de secondes permettent de générer une empreinte vocale unique qui, à la manière d'une empreinte digitale, identifie un fraudeur dès le premier appel dans 75% des cas. Un taux qui monte à plus de 80% au bout d'un an d'entraînement.

Quant à **Voice Biometrics**, cette technologie permet d'identifier des voix de fraudeurs connus intégrées dans une base de données en vue de faciliter leurs détections en environnement call-center.

Le machine learning au service de l'antifraude

Pour affiner son approche de filtrage, les technologies de Pindrop s'appuient sur des mécanismes de machine learning (branche d'exploration de l'intelligence artificielle).

« Plus on étaye les informations et mieux on est capable de détecter la fraude », assure notre interlocuteur. Un auto-apprentissage alimenté par la validation de l'entreprise utilisatrice.

Concrètement, à partir de ses analyses, Pindrop attribue un score de risque de fraude pour chaque appel.

Si un appel est jugé frauduleux, il est basculé vers une cellule antifraude qui valide, ou pas, la réalité de la tentative d'arnaque.

C'est cette validation qui vient alimenter vertueusement la base de fraudeurs mis en liste noire de Pindrop (exploitée via Voice Biometrics).

« Avoir une multitude d'informations par fraudeur nous permet de continuer à l'identifier même s'il change ses méthodes », assure notre interlocuteur. « *La voix est un élément supplémentaire pour étayer nos analyses.* «

Selon lui, le système ne générerait que 1% de faux positifs. En 2017, Pindrop a analysé plus de 1,1 milliard d'appels dans le monde.

La solution se concrétise derrière une appliance, une « blackbox » installée dans l'infrastructure du client pour intercepter les appels en temps réel sans impact sur le service.

A l'exception de la connexion au Pindrop Network (qui dispose d'un datacenter basé en Irlande pour couvrir l'Europe) pour vérifier la légitimité des numéros de téléphone, toutes les données sont traitées et stockées localement.

Aux Etats-Unis, la base de données des fraudeurs en liste noire peut être partagée dans le cadre d'un consortium public mais pas en France. *« La CNIL l'interdit »*, selon Vincent Pajot.

Au-delà du cercle de la finance et des banques

Pindrop appuie son modèle économique sur un contrat pluriannuel de trois ans calculé en fonction de la volumétrie des appels. Ses solutions sont distribuées par des intégrateurs (Dimension Data en Europe notamment) et directement par des fournisseurs d'infrastructures (Genesys).

« *Le retour sur investissement est réalisé entre quatre et six mois [pour un client, ndlr]* », assure Vincent Pajot. « *On économise des sommes astronomiques chiffrées en plusieurs millions d'euros par mois.* »

Les principaux clients de Pindrop sont les banques (7 des plus grands noms aux Etats-Unis) et les compagnies d'assurances, particulièrement ciblées par ces types de fraudes, ainsi que le secteur de la distribution.

Mais la technologie de l'entreprise peut potentiellement s'appliquer à d'autres domaines. Le porte-parole en France évoque les assistants vocaux amenés à piloter de plus en plus d'objets connectés, du boîtier domotique résidentiel à la voiture connectée.

Lire également
La façon de marcher, un moyen pour s'authentifier
Les mots de passe reconnus du bout des lèvres
La reconnaissance vocale de Microsoft fait jeu égal avec les humains

crédit photo © spe – shutterstock