Trackers

Description

Catégorie particulière de « mouchards », les *trackers* sont des logiciels nichés dans les applications mobiles. Ils participent à leur fonctionnement, notamment pour l'envoi des notifications, et servent également à adresser des messages publicitaires. Installés à l'insu de l'utilisateur à l'occasion du téléchargement d'une application, les *trackers* collectent une grande quantité de données personnelles.

Lancée en novembre 2017, la plateforme Exodus Privacy a été conçue pour porter à la connaissance des mobinautes l'existence de ces petits logiciels nichés dans les applications mobiles et qui captent leurs données personnelles. Elle a vu le jour à la suite d'une enquête journaliste sur la pratique marketing *drive-to-store*, dont les révélations ont motivé un groupe de hackeurs. C'est l'histoire d'une cause commune rondement menée dans l'univers opaque des adtech, un exemple de citoyenneté. Exodus Privacy est un modèle à suivre pour déjouer les *trackers*.

Tout commence par l'enquête du journaliste Corentin Durand, publiée en août 2017 sur le site d'information en ligne Numerama, menée auprès de l'entreprise parisienne Teemo (anciennement Databerries), spécialisée dans le *« drive-to-store »* (ou *« web-to-store »*) technique marketing visant à attirer les consommateurs vers un point de vente. Créée en 2014 par Benoît Grouchko, venu de Criteo (spécialiste français du ciblage publicitaire), François Wyss (anciennement chez Google) et l'entrepreneur spécialisé dans la technologie mobile Guillaume Charhon, Teemo compte ses clients dans les secteurs de l'automobile, de l'alimentaire, du bricolage ou de l'ameublement (Carrefour, Intersport, Leclerc, Casino, Leroy Merlin, Volkswagen…). Soutenue notamment par le fonds de capital risque Index Ventures (actionnaire historique de Criteo), Teemo a bénéficié d'une levée de fonds de 15 millions d'euros au printemps 2017. Avec une valorisation boursière de 50 millions d'euros, la start-up, promise à un bel avenir, s'attire les faveurs des personnalités de la high-tech qui y voient le « nouveau Criteo ».

Le journaliste de Numerama décrit la redoutable efficacité du service offert par Teemo :

— Le client de Teemo : *« Si je vous demande de me pister et de me dire où je suis, vous pourrez ? »*

— Teemo : *« Oui, donnez-moi votre IDFA »* [Identifier for Advertisers : série de chiffres servant à l'identification publicitaire des iPhone].

Une fois l'identifiant du client mouliné par les algorithmes dans la base de données de Teemo, s'affichent en quelques secondes sur une carte de la capitale les déplacements de ce dernier.

— Teemo : *« Vous êtes allé au restaurant hier soir ? »*.

Sans même disposer de l'IDFA, simplement à partir de son adresse et de son lieu de travail, il serait possible de retrouver n'importe quelle personne en cinq secondes, selon les informations communiquées au journaliste de Numerama, une arme potentielle pour les esprits malveillants.

Experte en *« real life targeting »* (ciblage dans la vraie vie), la start-up Teemo permet aux enseignes de cibler des consommateurs en fonction de leurs habitudes de fréquentation des points de vente et de leur transmettre des annonces commerciales sur leur téléphone portable lorsqu'ils se trouvent à proximité d'un magasin. La performance publicitaire correspond alors au nombre de visites effectuées sur le lieu de vente. Pour réaliser ce ciblage en temps réel, l'enquête du journaliste de Numerama a révélé que l'entreprise Teemo est en mesure de suivre près de 10 millions de Français, à intervalle de trois minutes, et à leur insu, grâce à la collecte des données de géolocalisation effectuée à partir des applications téléchargées sur leur téléphone portable.

Pour le moins intrusive, et surtout contraire aux règles relatives au respect de la vie privée, celles défendues par la Cnil, cette stratégie marketing implique trois catégories d'acteurs : les éditeurs d'applications mobiles, les annonceurs et les consommateurs internautes, ces derniers étant les seuls *« à ne pas être dans la confidence du pistage »*, précise le journaliste qui a découvert que Teemo avait développé un logiciel pour la publicité (un SDK, *Software Development Kit*) introduit dans une cinquantaine d'applications. Utilisé pour l'affichage (*display*), ce logiciel sert également à la collecte des données de localisation des mobinautes, envoyées toutes les trois minutes sur les serveurs de Teemo.

Parmi les éditeurs d'applications qui revendent les données de leurs clients à Teemo se trouvent notamment *Le Figaro*, *L'Equipe*, *Closer*, *Télé Loisirs* et *Météo France*. Cette collecte en continu des données de localisation des mobinautes clients des éditeurs n'apparaît pas dans les conditions générales d'utilisation (CGU) et soulève, en outre, la question de la responsabilité des éditeurs, puisqu'en l'espèce, c'est bien à eux, et non à Teemo, dont ils ignorent l'existence, que les mobinautes adressent, le cas échéant, l'autorisation de collecter leurs données personnelles. Le dirigeant de Teemo, Benoît Grouchko, se sert d'ailleurs comme d'un rempart pour sa société le fait que l'information des utilisateurs incomberait, selon lui, à ceux qui sont en relation directe avec la clientèle, en l'occurrence les éditeurs. Effectivement, sur le site de Teemo, ne figure aucune information. La société aurait reçu la visite de la Cnil avant l'été 2017.

L'histoire ne s'arrête pas là. Les révélations de Numerama, qui ont suscité de nombreuses réactions d'internautes, trouvent un certain écho dans la presse et provoquent même quelques remous au sein de Teemo, qui perd des contrats avec certaines agences de publicité. Surtout, la publication de cette enquête sur le réseau social décentralisé Mastodon va appeler la curiosité d'une hackeuse nommée U+039B, rapidement rejointe par d'autres férus du code. Ils vont bénévolement travailler d'arrache-pied pendant des mois afin de décortiquer une centaine d'applications sur Android, pour finir par découvrir qu'elles sont truffées de logiciels mouchards, discrets mais efficaces, appelés *trackers*, dont certains *« pesaient plus lourd en lignes de code que l'application en elle-même »*

, explique l'administrateur système du groupe qui se fait appeler Louis IX.

S'assurant le conseil de plusieurs avocats afin de ne pas franchir les limites de la propriété industrielle, les membres du groupe, qui s'activent autour de cette affaire en communiquant par *chat* crypté, se rencontrent pour la première fois à Paris en septembre 2017 et décident de créer une association le mois suivant. Ils ont trouvé le moyen de pister à leur tour les *trackers*, soit *« automatiser l'analyse du contenu et des émissions de données d'applications Android, à partir d'archives d'installation (APK) récupérées sur le Google Play Store »*, comme l'explique Guénaël Pépin du site NextInpact, qui suit les travaux du groupe depuis le début. Et ils comptent un nouvel allié avec le Privacy Lab de l'université américaine Yale qui s'est associé à leur recherche.

Les journalistes Guénaël Pépin, du site NextInpact, et Martin Untersinger du *Monde*, ainsi que le site britannique The Intercept, vont relayer le lancement par l'association de hackeurs, en novembre 2017, de la plateforme Exodus Privacy sur laquelle est publiée l'analyse de 375 applications. Résultats : une quarantaine de *trackers* différents ont été identifiés – et il y en a sans doute d'autres –, soit 2,5 en moyenne par application, certaines pouvant en compter une quinzaine. Prochainement, l'association offrira la possibilité de tester une application pour découvrir les *trackers* qu'elle contient et de créer une application Android chargée de signaler les *trackers* nichés dans les applications d'un téléphone portable. *« Entre nous, nous avons organisé une cause commune. Une cause qui a réuni des citoyens pendant trois mois, qui se sont entraidés et motivés pour réussir. Ça me donne de l'espoir et je dois dire que ça m'a surprise »*, a conclu U+039B. L'association espère trouver des soutiens afin de poursuivre son action.

Comme le détaille le journaliste Martin Untersinger, du *Monde*, dans son article annonçant le lancement d'Exodus Privacy, il existe trois types de *trackers* répertoriés par la plateforme :

- pour scruter l'utilisation d'une application par le mobinaute. Comme Xiti pour l'application du *Monde* , ces logiciels mesurent l'audience en comptabilisant notamment le nombre de pages visitées, leur enchaînement, le temps consacré et l'adresse IP. D'autres *trackers*, pour régler des problèmes techniques (*bug*), comme le logiciel Crashlytics (propriété de Google), récupèrent des informationssur le système d'exploitation mais également le numéro unique de l'appareil et parfois des données de localisation ;
- pour adresser de la publicité. DoubleClick, la régie de Google, collecte toutes sortes de données concernant l'appareil, l'historique de navigation et la géolocalisation, ou encore Ad4Screen qui sert à l'envoi de notifications dans les applications du *Monde*, du *Parisien*, de Voyages SNCF, de *Libération* , des Pages Jaunes, mais également, le cas échéant, au *retargeting* pour *« drainer du trafic en magasin et convertir les utilisateurs mobiles en acheteurs »* ;
- pour le *drive-to-store* que proposent, à l'instar de Teemo, les sociétés Vectaury et Fidzup. Cette dernière installe dans les magasins des box qui enregistrent l'identifiant de la carte réseau (appelé MAC) des téléphones portables dont le Wi-Fi est activé, pour pister leurs propriétaires dans les rayons et ensuite, grâce au *tracker* Fidzup présent dans des applications tierces, analyser leur navigation surle web, afin d'envoyer aux mobinautes des messages publicitaires les incitant à revenir au magasin.

On ne s'étonnera pas de voir figurer DoubleClick, le service publicitaire de Google, en tête des *trackers* les plus fréquemment embarqués dans les centaines d'applications passées au crible d'Exodus Privacy, ainsi que Crashlytics, utilisé par les développeurs. *« Par dizaines, ils se nichent dans des applications mobiles utilisées quotidiennement par des millions de Français. Ils capturent discrètement des données, souvent personnelles, sans que les utilisateurs en soient nécessairement conscients, alimentant au passage une industrie opaque et méconnue. Certains de ces acteurs disposent de données sur des millions de Français »*, écrit Martin Untersinger à propos des *trackers*. Et d'ajouter : *« En droit, la collecte de toute information directement liée à une personne ou à son appareil nécessite son consentement, y compris lorsqu'il s'agit d'une mesure d'audience. Peut-on parler de consentement lorsque l'utilisateur croit fournir ses données à une application et que dix ou quinze autres sociétés en profitent en sous-main ? »*

Désormais, de nombreuses enseignes ont installé des dispositifs pour récupérer les données de leurs visiteurs, comme le groupe Galeries Lafayette ou le centre commercial Quatre Temps situé en banlieue parisienne. Certaines l'indiquent à l'entrée, comme le BHV à Paris, d'autres pas. Concurrente de Teemo, l'entreprise Retency dit vendre à ses clients (Orange, Etam, C&A, Marionnaud, Leroy Merlin, Jardiland) *« le premier procédé de mesure universelle d'audience sur la voie publique »*. Concernant la mesure de fréquentation et l'analyse du comportement des consommateurs dans les magasins (géolocalisation au mètre près, durée, fréquence des visites…), un avis de la Cnil datant de 2014 précise pourtant que *« une information claire doit être affichée dans les lieux où sont mis en place ces dispositifs afin de garantir une réelle transparence vis-à-vis du public »*, que *« les données émises par le téléphone portable doivent être supprimées lorsque son porteur sort du magasin »* et que *« le consentement préalable et éclairé des personnes est nécessaire pour pouvoir conserver les données non anonymisées plus longtemps. »*

Si des entreprises comme Teemo ont eu toute liberté de prospérer en passant à travers les mailles du filet législatif ou réglementaire, il ne devrait plus en être ainsi à l'avenir. En débat à l'Assemblée nationale début février 2018, le projet de loi sur la protection des données personnelles, transposition du règlement européen sur la protection des données (RGPD, voir *La rem* n°42-43, p.21) devrait permettre de clarifier les pratiques. Engageant la responsabilité de tout acteur impliqué dans le traitement de données personnelles, cette nouvelle législation renforcera les dispositions existantes pour assurer une collecte licite, loyale et transparente – qui ne soit par ailleurs ni excessive ni disproportionnée – des informations sur les utilisateurs d'applications et de services connectés.

« Les entreprises adoptent des technologies de pointe comme les ultrasons ou les balises Bluetooth pour vous pister. Cela nous rapproche d'un monde à la Minority Report. *Il est souvent dit que les données collectées sont anonymisées, mais de nombreuses études montrent qu'il est facile de réidentifier un utilisateur si l'on dispose d'une riche base de données. L'idée selon laquelle la vie privée est préservée parce que les données sont anonymisées est fausse »*, expliquent au *Monde* Mike Kwet et Sean O'Brien, chercheurs associés au Yale Privacy Lab. *« Même si un utilisateur prend conscience de la présence de* trackers, *les options d'opposition à cette collecte sont problématiques.* […] *Le processus est complexe et il n'y a aucune garantie qu'il soit permanent. Mais il s'agit encore de « boîtes noires », et tirer tout cela au clair va nécessiter un sérieux travail d'enquête »* : un chantier en effet pharaonique avec le déploiement en cours des environnements connectés, domicile, voiture, ville entière.

Sources :

- Exodus Privacy, exodus-privacy.eu.org
- « Au BHV, et ailleurs, mieux vaut éteindre son téléphone portable pour éviter d'être pisté », Perrine Signoret, lexpansion.lexpress.fr, 3 août 2017.
- « Mesure de fréquentation et analyse du comportement des consommateurs dans les magasins », avis de la CNIL, cnil.fr, 19 août 2014.
- « Databerries, le « Criteo » du monde physique, lève 15 millions d'euros », Nicolas Rauline, *Les Echos* Entrepreneurs, LesEchos.fr, 21 mars 2017.
- « Enquête : comment les apps Figaro, L'Equipe ou Closer participent au pistage de 10 millions de Français », Corentin Durand, Numerama.com, 23 août 2017.
- « Les inconnues du dossier Teemo : quelques pistes pour poursuivre la réflexion », Corentin Durand, Numerama.com, 24 août 2017.
- « Rencontre avec Exodus Privacy, qui révèle les trackers des applications Android » Guénaël Pépin, NextInpact.com, 24 novembre 2017.
- « Des mouchards cachés dans vos applications pour smartphones », Martin Untersinger, LeMonde.fr, 24 novembre 2017.
- « Les mouchards des applications mobiles « nous rapprochent d'un monde à la Minority Report » », interview de Mike Kwet et Sean O'Brien, chercheurs associés au Yale Privacy Lab, propos recueillis par Martin Untersinger, LeMonde.fr, 24 novembre 2017.
- « Lutter contre les mouchards des apps, une cause citoyenne : voici l'histoire d'Exodus Privacy »,

Corentin Durand, Numerama.com, 8 décembre 2017.

Categorie

1. A retenir

date créée
6 avril 2018
Auteur
francoise