Un espion dans la poche

Par **Emilien Hofman**

C'est un fantasme presque immuable: nos smartphones seraient capables de nous espionner et, pire, de nous écouter. Sauf que la surveillance ne se fait pas toujours là où on le croit…

El Mahjoub Maliha se souvient d'un ressenti terrible. Ce lundi 1er novembre 2021, il consulte pourtant simplement ses e-mails sur son smartphone. Directeur des ventes de profession, ce Limbourgeois est par ailleurs un défenseur des droits humains du peuple du Sahara occidental, ce territoire en quête d'indépendance et opposé au Maroc, auquel il appartient officiellement. Ce jour-là, il a tout juste le temps de voir apparaître un message du secrétariat d'Etat des Etats-Unis sur son écran avant que ce dernier soit soudainement marqué comme «lu». Le vingtenaire confie alors son portable au laboratoire d'Amnesty International qui établit que cette infection est sans aucun doute un coup de Pegasus.

Ce logiciel développé par une entreprise privée israélienne doit alors sa réputation internationale à sa capacité à s'introduire dans un téléphone pour y récupérer des courriels, des photos, des contacts et même capter des appels en cours. A l'époque, les smartphones de Charles et Louis Michel sont également piégés par Pegasus. Mais le cas d'El Mahjoub pose question. Parce qu'il n'est pas la seule victime du piège. «Le danger concernait aussi ma famille, mes collègues et mes compagnons défenseurs des droits humains», témoigne celui qui a alors été approché par la police fédérale, mais qui attend toujours des réponses à ses questions: «Qui m'a ciblé, pourquoi, et où sont mes données volées?» En Belgique, il existe depuis 2021 une plateforme de communication ultrasécurisée destinée aux hauts fonctionnaires occupant un poste sensible. Mais cette protection n'est pas destinée au citoyen lambda tel qu'El Mahjoub Maliha. Alors, tous des proies?

Méthodes et objectifs différents

Installer un traqueur sur un téléphone portable peut, de fait, s'avérer relativement facile. «Cela peut être un logiciel implanté manuellement en quelques clics par

GETTY

Installer un traqueur dans un téléphone est relativement facile, en quelques clics.

le conjoint, l'employeur, le collègue d'une personne qui laisse son appareil libre quelques minutes», révèle Guillaume Deterville. Le fondateur et directeur technique –pas encore trentenaire– de la société de cybersécurité Cresco s'est fait connaître à 17 ans en piratant le site officiel de l'Enseignement.

Aujourd'hui reconverti en «hacker éthique», le Bruxellois pointe une deuxième forme d'implantation de traqueurs, appelée «one clic». «Il s'agit de piéger un utilisateur en l'amenant à cliquer sur un lien qui ouvrira un pop-up capable d'installer automatiquement un logiciel de suivi», détaille-t-il. «La majorité des téléphones modernes vont bloquer ces téléchargements malicieux. Par conséquent, ces attaques sont plutôt réalisées par des services de renseignement ou des gens très calés.» La troisième méthode d'installation ciblée par l'expert en cybersécurité est celle dite du «zero clic». Elle touche les vulnérabilités qui ne sont pas encore connues par les constructeurs. Elle se vend donc parfois à plusieurs millions de dollars parce qu'elle permet d'attaquer à distance un téléphone rien qu'en disposant du numéro, pour y faire ensuite à peu près ce que l'on veut. Çà et là, il apparaît régulièrement qu'en cas d'infection, le téléphone peut surchauffer ou avoir une consommation excessive de batterie, sortir sans raison du mode veille, envoyer des messages étranges aux contacts ou encore émettre certains bruits déconcertants pendant les appels. «Si le logiciel est bien conçu, sa communication de données sera pratiquement indétectable», **...**

… expose Jean-Michel Dricot, expert en cybersécurité à l'ULB. «L'utilisateur non initié détecte difficilement un logiciel malveillant, mais il peut agir en effectuant régulièrement des mises à jour, qui permettent de s'en débarrasser.»

Guillaume Deterville distingue trois types de desseins de ces espionnages. Le premier est d'ordre politique. «Tous les gouvernements du monde ont la possibilité de mettre les gens sur écoute pour des raisons de sécurité, assure-t-il. Ils passent un accord avec un opérateur qui leur donne accès à des relevés de pylônes téléphoniques, indispensables pour capter la plupart des communications. Seuls les messages chiffrés sont beaucoup plus difficilement détectables.» Il y a quelques années, les médias internationaux ont beaucoup relayé l'existence des IMSI-catchers. Ces valises dotées d'un ordinateur portable, d'une antenne et d'une batterie sont considérées comme des antennes-relais par les GSM et permettent donc d'intercepter toute communication téléphonique dans un rayon pouvant atteindre plusieurs centaines de mètres. «C'est du matériel exclusivement réservé au renseignement, mais quelqu'un qui se débrouille bien techniquement pourrait en fabriquer… bien que ça soit très illégal», commente Guillaume Deterville avant de détailler le deuxième type d'espionnage, celui dit «privé». «Cela correspond à la volonté d'enregistrer confidentiellement les informations de l'activité téléphonique d'une autre personne, par exemple pour savoir ce que fait son conjoint.» Le stalkerware est l'outil principal qui rend cette surveillance possible en enregistrant les appels téléphoniques, en extrayant des données, en accédant à la localisation ou en déclenchant à distance le micro ou la caméra… «Enfin, il y a l'espionnage "marketing", glisse le hacker éthique. Et là, il y a pas mal de choses à dire… »

Oreille attentive

Encore un peu plus depuis ce jour de février dernier, quand le journal *Le Monde* annonce qu'Apple serait visé par une plainte provenant de la Ligue des droits de l'homme pour violation de la vie privée, traitement illicite des données personnelles et pratique commerciale trompeuse. La marque à la pomme est alors accusée par un ancien salarié d'effectuer des enregistrements à l'insu des utilisateurs. Passé par le service d'analyse du contenu des enregistrements de l'assistant virtuel Siri, Thomas Le Bonniec explique avoir eu accès dans le cadre de son travail à des captations de conversations privées concernant des états de santé ou des opinions politiques, et même à des moments aussi intimes qu'une relation sexuelle. Alors qu'Apple vient de payer 95 millions de dollars quelques jours plus tôt pour mettre fin à une plainte sur la confidentialité des données, cette affaire ne manque pas de galvaniser ceux qui croient à la réalité d'un espionnage marketing illégal par écoute. Michele Rignanese n'en fait pas partie. «Aucune preuve formelle de l'existence de ce type de surveillance n'a été dévoilée», jette ce dernier, porte-parole du Centre pour la cybersécurité Belgique (CCB). «D'un point de vue technique, c'est fortement improbable: cela supposerait que l'appareil envoie en permanence des données dans le cloud, ce qui demanderait des ressources énergétiques inimaginables vu le nombre d'utilisateurs.» D'autres observateurs ajoutent que la voix étant considérée comme une donnée personnelle, son utilisation sans consentement exposerait ses exploitants à de lourdes sanctions.

Comment expliquer, dès lors, l'incontournable apparition de publicités sur le fil

«Effectuer régulièrement des mises à jour permet de se débarrasser de logiciels malveillants.»

GETTY

L'Imsi-catchern trompe le GSM, qui le considère comme une antenne-relais, permettant ainsi l'interception d'une communication.

d'actualité de réseaux sociaux à propos d'un produit ou d'une destination de vacances justement évoqué(e) oralement peu de temps auparavant? Pour la plupart des spécialistes, il y a d'abord une question de biais cognitif qui fait oublier l'existence des traces laissées suite à une recherche antérieure. Cela peut aussi être dû à l'exploitation et le recoupement d'une multitude de données. Il suffit ainsi qu'une personne se connecte à la borne wifi d'un ami, puis qu'elle fasse une recherche commerciale en rentrant chez elle pour que des logiciels liés aux réseaux sociaux en déduisent qu'il y a probablement eu discussion à ce sujet et qu'ils envoient une annonce à l'ami en question.

Mieux, si l'on peut dire: certaines applications analysent les itinéraires Google Maps, le temps passé sur certaines publications et consultent même l'historique de navigation. «Je ne vois pas pourquoi les entreprises s'embêteraient à écouter des heures entières de contenu audio, enfonce Michele Rignanese. Elles disposent déjà de suffisamment d'informations en récoltant des détails ultra-précis grâce aux cookies et à la cession de données personnelles dans les applications.» Et ce n'est pas tout: beaucoup d'entreprises comme Meta font du commerce de métadonnées, soit les infos sur les datas, leur fonds de commerce. Lors d'un achat en ligne, les métadonnées renseignent par exemple sur le site Web, la carte de crédit utilisée, la gamme ou le montant du produit. «De nombreuses firmes ont compris que ces métadonnées apportent autant voire plus d'informations que les données, avance Jean-Michel Dricot. Elles sont également moins énergivores en temps d'analyse et ne sont pas protégées par la loi.»

Le micro de la SNCB

Parce qu'il sait que ça ne manque jamais d'impressionner son public, la «démonstration» est devenue la première étape des ateliers InformEthique que François Dossogne organise au sein de l'asbl Les Amis de la Terre. «Le but est de montrer aux participants que ce qu'ils ont dans la poche est en train de les fouiller», sourit cet ancien militaire de carrière, qui prend cette fois-ci au hasard l'exemple de l'application SNCB. «Si j'accepte ses conditions d'utilisation, je donne accès à ma géolocalisation –ça a une logique pour que l'app sache dans quelle gare je me trouve quand je lance une recherche–, à mon appareil photo –pratique aussi pour scanner les QR codes–, mais également au micro... Pourquoi? On pourrait imaginer que l'app écoute.» Le militaire à la retraite ajoute que le programme de l'opérateur ferroviaire public a accès en lecture au carnet d'adresses et en écriture à l'agenda, à la carte mémoire, donc aux photos –«mouais»–, et peut aussi modifier les paramètres. «Cela pose d'autant plus question que cette app est reliée à des services de pistage et que personne ne peut contrôler ce qui est transmis.» Via le site Web des spécialistes du code Exodus Privacy, François Dossogne dénonce effectivement la présence de six services de pistage connus: deux pour Facebook, deux pour Google, un pour Adobe et un autre pour Instabug. La SNCB est-elle au courant? «Pas sûr, rétorque-t-il. Il s'agit d'un échange de services classique: l'entreprise paie des informaticiens pour développer son app, mais elle reprend des logiciels tout faits d'identification de la personne chez Google.» ...

Pour raison de sécurité, n'importe quel gouvernement peut mettre un quidam sur écoute. Seuls les messages chiffrés sont difficilement détectables.

GETTY

La géolocalisation, outil utile pour renseigner. Mais outil de pistage également…

… L'animateur des ateliers InformEthique estime que le consommateur paie de ses données le trop grand laxisme des autorités belges à l'égard du RGPD. «Tout un flux d'informations remonte en échange de services dits "gratuits", avance-t-il. Toutes ces données sont collectées et raffinées chez des courtiers en données qui les revendent ensuite à des assureurs, des banques, des agences de publicité ciblée…» Google possède en outre les autorisations légales pour fouiller les e-mails à des fins marketing, les croiser avec les photos du Drive et les recherches YouTube avant de soumettre à l'usager une publicité parfaitement réfléchie.

DéGoogliser?

Plus un smartphone regorge d'applications, plus il risque d'être suivi par des traqueurs publicitaires. «Il suffit alors de recouper les données personnelles pour ouvrir la porte d'une gigantesque mine d'informations et des faiblesses de l'usager», prévient Michele Rignanese, du CCB. En 2022, le centre a donc lancé une grande campagne intitulée «OK n'est pas toujours OK» pour sensibiliser à l'importance de la prudence numérique. «Le premier conseil consiste à télécharger uniquement des applications issues de magasins officiels, débute le porte-parole. Nous recommandons également de ne jamais ignorer les alertes de sécurité, d'effectuer les mises à jour et de rester frileux par rapport aux autorisations: une application météo n'a pas besoin d'accéder à l'appareil photo.» Devant les classes d'élèves qui se succèdent lors des cycles d'Inform Ethique, François Dossogne propose quant à lui de «déGoogliser» les téléphones, «parce que Google installe une sorte de coque imperméable qui empêche l'utilisateur de contrôler Android et de garder le dernier mot», soutient-il. Moyennant une petite manipulation technique et l'imposition faite au smartphone de procéder à l'installation malgré ses probables réticences, il suffirait ainsi de placer un logiciel libre qui n'imposerait aucune restriction à l'usage et ne contiendrait pas de traqueur de vie privée. «Mais il est impossible d'installer un système alternatif sur iPhone. Des firmes comme BlackBerry se sont néanmoins spécialisées dans le commerce de téléphones ultrasécurisés.»

Certaines applications analysent jusqu'aux itinéraires Google Maps.

GETTY

Menaces sur la démocratie

Reste à voir si toutes ces précautions resteront valables dans un futur proche… Dans un article publié dans *The Financial Times*, la docteure en psychologie sociale Shoshana Zuboff s'inquiétait, en 2019, des dérives qu'elle attribuait au «capitalisme de la surveillance», qui s'étendrait au-delà du secteur du numérique pour toucher ceux de l'assurance, du commerce de détail, de la santé, de la finance, du divertissement ou encore de l'éducation. «Les capitalistes de la surveillance produisent ainsi des asymétries profondément antidémocratiques en matière de connaissance et de pouvoir découlant de cette connaissance. Ils savent tout de nous, et font tout pour que nous ne sachions absolument rien de leurs pratiques. Ils prédisent notre avenir et manipulent notre comportement, mais pour le compte de tiers qui en tireront un profit financier ou l'exploiteront à leurs fins.»

En France, on discute régulièrement de la possibilité d'activer à distance des appareils électroniques, comme des smartphones, à des fins d'enquête, ou d'obliger des plateformes de messagerie cryptée telles que Signal et WhatsApp à autoriser l'accès aux correspondances des narcotrafiquants. «Avec la montée de l'extrême droite, le narcotrafic, le cyberharcèlement, etc., l'Etat cherche absolument à savoir qui est qui sur toutes les plateformes, théorise François Dossogne. Nos politiciens ne se rendent pas bien compte que de cette façon, ils sont en train de mettre en place une forme d'Etat policier qui n'est pas bon pour la démocratie…» En Belgique, l'utilisation de plus en plus fréquente d'applications à communication chiffrée complique les missions d'interception ciblée des forces de l'ordre, mais aucun travail parlementaire n'est jusqu'ici parvenu à proposer une solution qui maintiendrait l'équilibre entre la protection de la vie privée et lapossibilité pour un Etat démocratique de capter des communications dans le cadre d'enquêtes. «Toute la difficulté consiste à savoir où mettre le curseur, note Jean-Michel Dricot, de l'ULB. La technologie a toujours été un amplificateur: si l'on commet des erreurs en écoutant des conversations à la demande de la police, cela peut ouvrir un certain nombre de portes dérobées. Et mener à des conséquences dramatiques.» ●

«Aucune preuve formelle de l'existence de l'espionnage marketing illégal par écoute n'a été dévoilée.»