Selon Edward Snowden « ce que l'on voit maintenant, c'est une industrie créée pour pirater les smartphones. Ces gens prennent le plein contrôle du téléphone et le retournent contre la personne qui l'a acheté mais ne le possède plus vraiment. » © REUTERS.

ENTRETIEN

PAUL LEWIS (« THE GUARDIAN »)

Huit ans après ses révélations concernant la surveillance de masse par les services de renseignement américain, le lanceur d'alerte Edward Snowden accorde un entretien au Projet Pegasus, pour réagir aux révélations de ce consortium de seize médias, dont *Le Soir*. Pour lui, l'utilisation de ce genre de logiciel est une menace grandissante dont on doit se prémunir en changeant les lois.

Quelle est votre première réaction en découvrant les révélations du Projet Pegasus ?

C'est évidemment choquant. On découvre des journalistes, des chefs d'Etat, des opposants politiques, des militants des droits de l'homme, c'est terrible. J'ai toujours soupçonné que ces outils de surveillance étaient utilisés de façon abusive. On l'a vu en 2013, mais c'était exclusivement par des gouvernements, avec des outils « maison », s'appuyant sur des fournisseurs de service privés. Il y avait un voile de légitimité et de légalité des procédures. Ce n'était déjà pas suffisant mais c'était là.

NSO Group représente un autre type de marché de logiciels malveillants. Il ne se soucie pas de la loi et des réglementations. Il vend à n'importe quel client jugé fiable, dont il pense qu'il ne leur créera pas de problèmes. NSO dit : « Nous ne savons pas quel usage ils font (de Pegasus), nous n'en sommes pas responsables, nous vendons et ils signent un contrat qu'ils respectent, et s'ils ne le respectent pas, ce n'est pas vraiment notre problème, parce que ce sont eux qui enfreignent le contrat. »

C'est une industrie qui ne devrait pas exister. Nous voyons NSO Group parce que c'est la vedette de cette industrie. Mais ce n'est qu'une entreprise au milieu de beaucoup d'autres. Et si une seule entreprise pose autant de problèmes, qu'en est-il des autres ? Ce que le Projet Pegasus révèle, c'est que ce secteur ne commercialise que des outils d'infection. Ils ne vendent pas de produits destinés à la sécurité, ne fournissent aucune protection, aucun remède. Ils ne produisent pas de vaccins, ne vendent que le virus.

> *Il faut un moratoire mondial sur le commerce des failles logicielles et des outils exploitant ces failles*

Par le passé, vous avez décrit les smartphones comme « un espion dans votre poche ». Pensez-vous que ces révélations le confirment ?

Je pense que c'est pire. Quand je parlais d'espion dans votre poche, je pensais au fait que ces objets communiquent avec un réseau téléphonique, et suivent votre géolocalisation. Que vous avez Facebook, qui vous espionne aussi. Mais ce sont essentiellement des programmes à but commercial. Ce que l'on voit maintenant, c'est une industrie créée pour pirater ces smartphones, et aller au delà de ce que l'on savait exister. Ces gens prennent le plein contrôle du téléphone et le retournent contre la personne qui l'a acheté mais ne le possède plus vraiment. Et il faut se rappeler que ces téléphones sont des clones. Les iPhones, par exemple, tournent avec le même logiciel dans le monde entier. S'ils trouvent le moyen de pirater un iPhone, ils ont le moyen de tous les pirater. Et c'est ce qu'ils font, et ce qu'ils vendent. C'est une attaque consciente et intentionnelle contre une technologie sur laquelle tout le monde se repose. Peu importe votre drapeau, votre langue, tout le monde est concerné.

L'ancien rapporteur des Nations unies pour les droits de l'homme, David Kaye, a déclaré que l'industrie de la surveillance était hors de contrôle, qu'en pensez-vous ?

Absolument. Le commerce de la surveillance existait déjà dans le passé. Des entreprises ont fabriqué et vendu des mouchards, comme des micros déguisés. Mais ces micros sont achetés par des gouvernements, puis par la police locale, et les agents doivent les installer physiquement dans un domicile, une voiture, un bureau, et doivent probablement demander un mandat judiciaire. C'est difficile et coûteux, et c'est donc utilisé en cas de réelle nécessité, et de façon proportionnée. Mais s'ils peuvent faire la même chose, à moindre coût et sans aucun risque, ils vont se mettre à le faire tout le temps, contre toute personne présentant un intérêt, même marginal. C'est ce que montre cette liste de 50.000 personnes sélectionnées. Vous ne pouvez pas installer des micros dans 50.000 foyers, il n'y a pas assez de spécialistes en écoutes dans tous ces pays pour ça. Mais s'ils peuvent simplement tendre le bras et accéder à votre poche, ils le feront.

Vos révélations ont mis en lumière les capacités de la NSA et du GCHQ. Pensez-vous que ces gouvernements auraient la capacité d'effectuer ce type d'espionnage sans l'aide de l'industrie de la sécurité privée ?

Cela dépend des pays. Beaucoup de pays autoritaires, comme le Kazakhstan, l'Ouzbékistan ou le Barhein, ont des sociétés très fermées, peu ouvertes au développement technique, et c'est difficile pour eux de produire ces capacités. Mais s'ils peuvent simplement payer quelqu'un d'autre pour leur fournir ce service, tout est à leur portée.

Si ces entreprises n'existaient pas, quelle serait l'alternative ? Ces gouvernements diraient-ils simplement : on ne peut espionner personne, on ne peut pas poursuivre nos enquêtes, on ne peut pas rechercher les criminels et les terroristes ? Bien sûr que non. Ils embaucheraient leurs propres développeurs, travailleraient en interne et développeraient leurs propres outils, ça serait difficile et coûteux. Ça serait aussi inefficace. Et c'est ce que nous voulons.

Qui devons-nous tenir pour responsable ? L'entreprise privée ou le gouvernement qui utilise son logiciel espion ?

Les deux, évidemment. Mais il ne s'agit pas seulement de se demander qui tenir responsable, par exemple en Israël ou au sein de cette entreprise en particulier. Il faut un moratoire mondial sur le commerce des failles logicielles et des outils exploitant ces failles. Il faut néanmoins le faire en protégeant la recherche, et en interdisant avant tout le fait de tirer un profit pécuniaire de ce marché. Si NSO Group ne peut plus faire de profits, ils mettent la clé sous la porte demain, et c'est pareil pour toutes les entreprises de cette industrie.

> *La seule façon de lutter est de changer les lois qui permettent à ces entreprises d'opérer et de commercer*

Il y a une autre question, plus générale, que nous devons nous poser, que l'Europe et les Etats-Unis doivent se poser. Comment ces entreprises ont-elles pu rencontrer un tel succès commercial et avoir une telle assise dans le monde, si ce n'est du fait de l'échec des réglementations en place ? Le régime actuel de contrôle des exportations a échoué à contrôler l'impact de l'industrie des logiciels malveillants.

Qu'attendez-vous désormais ?

L'inaction n'est plus une option. Si l'on ne fait rien pour arrêter la vente de cette technologie, ça ne sera pas juste 50.000 cibles, mais 50 millions, et cela arrivera bien plus vite que l'on peut s'y attendre. On ne veut pas interdire les recherches (sur la sécurité informatique et les failles logicielles, NDLR). La recherche peut être utilisée pour sécuriser nos appareils, les rendre plus sûrs. Mais quand ces technologies sont vendues dans un but offensif, ou vendues tout court, c'est là que l'on voit des acteurs malintentionnés arriver dans cette industrie.

Que peuvent faire les gens pour se protéger ?

Que peuvent faire les gens pour se protéger des armes nucléaires ? Des attaques chimiques ou bactériologiques ? Il y a certaines industries, certains secteurs, contre lesquels il n'y a pas de protection, et c'est pour ça que nous limitons la prolifération de ces technologies. Nous n'autorisons pas le commerce d'armes nucléaires, chimiques ou bactériologiques. Mais nous ne faisons rien contre ces outils numériques. Nous devons mettre fin à la vente de ces technologies intrusives, c'est la seule façon de nous protéger.

Beaucoup de gens lisent ces révélations, écoutent ce que vous dites, mais ne veulent pas se séparer de leur téléphone, comment faire ?

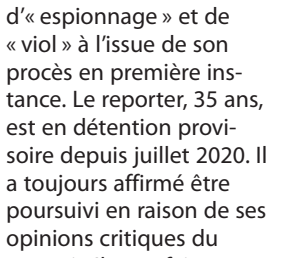
Vous ne devriez pas avoir à abandonner votre téléphone. C'est tout le problème. Ces entreprises sont extrêmement prédatrices. Peu importe qui vous êtes et ce que vous faites, peu importe votre position, cela ne vous protégera pas. Vous êtes ministre, ou Premier ministre ? Vous êtes sur la liste. Un juge de la cour suprême ? Vous êtes sur la liste. Vous êtes une personne ordinaire ? Vous êtes sur la liste aussi. Tout ce qu'il vous faut, c'est attirer l'attention de quelqu'un avec assez d'argent pour acheter auprès d'une de ces entreprises les outils pour pirater votre téléphone. Apple et Google, s'ils ne sont pas les acteurs les plus vertueux de la planète, font néanmoins de leur mieux pour lutter contre ces technologies, mais c'est un combat inégal. En face, on a des entreprises milliardaires qui se consacrent à chercher des moyens de pénétrer par effraction dans des appareils. Ils trouveront un moyen d'entrer. On ne peut pas dire aux gens « Vous devez vivre comme un espion ou un lanceur d'alerte » simplement pour pouvoir utiliser un smartphone. C'est ridicule, ce n'est pas la bonne solution. La seule façon de lutter est de changer les lois qui permettent à ces entreprises d'opérer et de commercer.

Traduction par Florian Reynaud (« Le Monde »)

Le journaliste Omar Radi condamné à six ans de prison

Un tribunal de Casablanca a condamné lundi le journaliste et défenseur des droits humains Omar Radi à six ans de prison dans une double affaire d'« espionnage » et de « viol » à l'issue de son procès en première instance. Le reporter, 35 ans, est en détention provisoire depuis juillet 2020. Il a toujours affirmé être poursuivi en raison de ses opinions critiques du pouvoir. Il peut faire appel. L'enquête pour « espionnage » avait été ouverte fin juin 2020 après la publication d'un rapport d'Amnesty International affirmant que le téléphone de M. Radi avait été piraté via le logiciel Pegasus de la firme israélienne NSO. M. Radi était accusé d'« atteinte à la sécurité intérieure de l'Etat » et d'avoir reçu des « financements étrangers » en lien avec « des services de renseignement » mais aussi de « viol ». Il a toujours nié ces accusations.

AFP



Omar Radi, en mars 2020. © REUTERS.

ABONNÉS
LE SOIR
A lire sur notre site, « Au Maroc, la répression s'aggrave contre les voix libres », par Baudouin Loos
plus.lesoir.be