Attentats de Paris : WhatsApp et Telegram ont été utilisés par les terroristes

Selon CNN, certains des terroristes impliqués dans les attaques du 13 novembre ont utilisés des applications de messagerie chiffrée pour préparer ces attentats. La chaîne américaine, qui cite des sources officielles proches de l'enquête, explique notamment que Telegram et WhatsApp, service aujourd'hui dans le giron de Facebook, auraient été employés à cette fin. Tous deux fournissent un chiffrement de bout en bout difficile à percer par les services de sécurité. Selon les sources de nos confrères, ces applications, présentes sur certains des smartphones retrouvées sur les scènes de crime, auraient été employées pour des communications entre terroristes avant les attaques. Le contenu de ces échanges étant chiffré, il n'est pas sûr que les enquêteurs y aient un jour accès, précise CNN.

Bien qu'imprécises, ces affirmations constituent le premier lien officiellement établi entre les messageries chiffrées et la préparation des attaques de Paris. Certes, après les attentats, Telegram, un service fondé par deux frères russes, défenseurs de la liberté d'expression, avait été mis en cause pour sa passivité à l'égard de l'Etat islamique. Mais cette accusation ciblait les canaux de diffusion proposés par Telegram et exploités par le groupe terroriste pour propager ses messages. A la suite des attentats du 13 novembre, 78 canaux de diffusion du groupe terroriste, diffusant en 12 langues différentes, ont été fermés par Telegram.

Telegram : filtrage minimum

Reste la fonction centrale de cette application : l'envoi gratuit de messages chiffrés de bout en bout à n'importe quel autre utilisateur du service (sur iOS, Android, Windows Phone, PC, Mac OS X). Ces messages peuvent également s'effacer après une certaine durée, des deux côtés de la communication. Dans ce mode (secret chat), Telegram n'est pas en possession des moyens permettant de décoder les données transitant sur ses serveurs. Le service précise d'ailleurs qu'il ne répond pas aux demandes des autorités portant sur les chats et les chats de groupe. A ce jour, seuls les canaux de diffusion (channels), les robots (bots) et les stickers sont filtrés, selon les affirmations de la société.

C'est bien sur ce point que se cristallise aujourd'hui le débat entre, d'un côté, les services de sécurité et, de l'autre, les défenseurs des libertés publiques et les industriels de l'IT. Suite aux révélations d'Edward Snowden et de peur de voir les utilisateurs se détourner de leurs technologies, les industriels ont mis en place des techniques de chiffrement contrôlées par les utilisateurs eux-mêmes. Au-delà des multiples messageries offrant du chiffrement de bout en bout (WhatsApp et Telegram n'étant que deux exemples), Apple et Samsung, les deux leaders des terminaux mobiles, ont embarqué ce type de technologies au cœur de leurs smartphones. Même en cas de requête officielle des services de police, les deux géants affirment ne pas être en mesure de dévoiler le contenu des communications de leurs utilisateurs, faute d'être en possession de la clef permettant de déchiffrer ces échanges.

WhatsApp bloqué au Brésil

En France, tout récemment, la Direction des libertés publiques et des affaires juridiques, un service dépendant du ministère de l'Intérieur qui prépare deux projets de loi (l'un sur l'état d'urgence, l'autre sur l'anti-terrorisme), a intégré dans ses recommandations le blocage de Tor (anonymat sur Internet), l'interdiction des points d'accès WiFi publics et l'obligation d'intégrer des backdoors pour les applications de VoIP comme Skype. Même si elles ont été écartées par l'exécutif, ces options montrent bien que les services en charge de la lutte contre le terrorisme tentent de faire bouger les lignes sur le chiffrement. Au Brésil, WhatsApp a été bloqué par les opérateurs pendant quelques heures cette semaine, une mesure de rétorsion après que la messagerie a refusé de coopérer dans le cadre d'une enquête criminelle.

Mais c'est aux Etats-Unis que le débat est le plus vif et a le plus de chance d'avoir une réelle portée. C'est en particulier le FBI qui mène la charge contre le chiffrement fort. Cette semaine encore, son directeur, James Comey, a assuré, lors d'une conférence sur le terrorisme à New York, que « *l'utilisation du chiffrement est au cœur des techniques terroristes* ». Le FBI explique notamment n'être pas parvenu à décoder 109 messages échangés entre un terroriste et un correspondant en Syrie, connu pour être affilié à Daech, avant l'attentat de Garland, au Texas, en mai dernier. Malgré les pressions de l'appareil de sécurité américain, aucun fournisseur n'a – officiellement du moins - accepté à ce jour d'affaiblir ses méthodes de chiffrement pour être en mesure de répondre aux requêtes des forces de l'ordre.

Des OS, des messageries, des outils dédiés…

Pour y parvenir, Apple et Samsung seraient forcés de modifier l'OS de leurs smartphones. Depuis iOS 8 et Android 5.0 (Lollipop), les clefs de chiffrement sont en effet embarquées directement sur les terminaux, donnant aux utilisateurs un contrôle total sur leurs outils. Par ailleurs, obtenir une porte d'entrée sur les systèmes d'exploitation mobiles ne permet pas de traiter la question des messageries chiffrées ou d'outils de chiffrement complémentaires. Plusieurs medias outre Atlantique expliquent ainsi que les auteurs des attentats de Paris et de San Bernardino ont également employé un outil de chiffrement pour Windows, Mujahedeen Secrets 2, créé en 2007 par des développeurs anonymes pour les besoins de Al-Qaeda.

De leur côté, les experts en sécurité expliquent qu'introduire des portes dérobées dans les outils de sécurisation des échanges ne ferait que réduire la sécurité globale d'Internet. Dans un récent rapport du MIT, une quinzaine de chercheurs (dont le gourou de la sécurité Bruce Schneier) expliquaient : « *La complexité d'Internet aujourd'hui, avec des millions d'apps et de services connectés globalement, signifie que les exigences des forces de l'ordre vont probablement introduire de nouvelles failles de sécurité, non anticipées et difficiles à détecter.* »

A lire aussi :

Le procureur de Paris prend position contre le chiffrement des smartphones

WiFi interdit, Tor bloqué, backdoors : les services de police en roue libre

Après les attentats : faut-il mieux encadrer le chiffrement ?

Crédit photo : Denys Prykhodov / Shutterstock