on hors norme pour piéger les narcos

viennent à cartographier de possibles réseaux criminels et à identifier de premiers suspects.

Lors de cette première phase aussi, les noms de groupes de discussion, non codés, sont interceptés. Et éveillent la suspicion des policiers, soit parce que leurs membres bornent le long de l'estuaire de l'Escaut, ou parce que les noms de ces groupes font penser à des activités illégales : « 50st afgeven » pourrait renvoyer à l'enlèvement de 50 paquets de cocaïne, « 1700 » faire référence à un enlèvement sur le quai 1700, « Cartagena » renvoie possiblement à la ville colombienne de Carthagène…

« A table avec les criminels »

En mai et juin 2020 enfin, sans que les administrateurs de Sky ECC et leurs clients se doutent de quoi que ce soit, le piège se referme : munis de nouveaux mandats décernés à Lille, les policiers procèdent à deux captures de la mémoire vive du serveur principal logé chez OVH, ce qui leur permet de mieux comprendre encore le fonctionnement de la messagerie et de recueillir de premières clefs de chiffrement, indispensables sésames à une lecture « en clair » des communications. Mais encore faut-il être en mesure d'intercepter tous les échanges et toutes les clefs en temps réel : les policiers procèdent ainsi à ce qu'ils appellent la technique de « l'homme du milieu ». Un serveur pirate est placé à côté du serveur officiel de la société canadienne, le rôle de cette boîte noire étant de collecter et d'archiver tous les échanges avec les abonnés de Sky ECC. Lorsque l'un de ceux-ci entame une communication, son application se connecte au serveur de Roubaix et de manière invisible, reçoit une notification qui l'incite à libérer toutes les clefs nécessaires au décodage de la conversation. Sans que les utilisateurs de l'application et les administrateurs ne se rendent compte de quoi que ce soit. « Un collègue néerlandais a dit que c'était comme si nous étions à table avec les criminels », confie la directrice générale d'Europol, Catherine De Bolle. « Et c'était vraiment ça. Nous avions toutes les informations dont nous avions besoin à ce moment-là. »

Durant trois semaines, du 15 février au 6 mars 2021, les autorités observent ainsi en direct les criminels s'échanger des messages et des photos, évoquer des enlèvements, des règlements de comptes, des livraisons de stupéfiants, des braquages. Plusieurs possibles meurtres seront ainsi évités : un assassin péruvien devait être embauché pour tuer une famille allemande, une attaque à l'explosif était planifiée à Francfort, un Néerlandais résidant en Colombie et un juge monténégrin devaient être assassinés… « Je pense que nous avons évité 114 meurtres », estime Catherine De Bolle.

Le 9 mars 2021, c'est le coup de grâce. « Ce matin, dans un dossier du parquet fédéral, plus de 200 perquisitions ont été menées et 48 personnes ont été privées de liberté et emmenées pour audition », communique le procureur fédéral belge, Frédéric Van Leeuw. « Plus de 1,2 million d'euros, quinze armes prohibées, dont six armes à feu, huit véhicules de luxe, trois machines servant à compter l'argent, des uniformes de police et des balises GPS ont été également saisis ce jour. »

Le 10 mars, alors que s'enchaînaient auditions et interpellations, un avertissement sur le site de la messagerie tentait de rassurer : « La plateforme Sky ECC reste sécurisée et aucun appareil Sky ECC autorisé n'a été piraté. »

Un peu plus tard, toutes les données interceptées étaient mises sous scellés, les noms de domaines saisis par le FBI et, en Belgique comme ailleurs, la phase judiciaire ne faisait que débuter. Fin octobre 2021, 1.100 policiers menaient une centaine de perquisitions dans le pays sous la direction d'un juge bruxellois, démantelant six laboratoires d'extraction de cocaïne, saisissant des armes à feu, des voitures de luxe et même un moteur de propulsion de (petit) sous-marin. A ce jour et consécutivement au décryptage de Sky ECC, plus de 1.000 condamnations ont été prononcées en Belgique, pour la plupart des narcotrafiquants. La cour d'assises de Paris, elle, devrait voir comparaître – vraisemblablement l'an prochain – des responsables de l'entreprise canadienne Sky Global et une série d'intermédiaires.

(1) Jean-Francois Eap s'exprime pour la première fois sur cette affaire dans le documentaire *La messagerie du crime*, réalisé par nos partenaires Guillaume Dasquié et Nicolas Jaillard. Il sera diffusé par la RTBF ce mercredi 20 novembre.

Une structure pyramidale

Le fondateur. Né en 1985 de parents cambodgiens qui ont fui le régime des Khmers rouges vers le Canada, Jean-François Eap a étudié l'informatique mais a quitté prématurément l'université pour se lancer dans l'entrepreneuriat : il a d'abord travaillé pour Rogers Communications, un des géants des télécommunications au Canada, avant de racheter les magasins pour lesquels il travaillait. En 2010, il crée Sky Global et la messagerie Sky ECC avec l'objectif d'offrir une sécurité maximale aux utilisateurs. Inculpé aux Etats-Unis pour avoir participé à une entreprise criminelle qui facilitait le trafic de stupéfiants et en France pour blanchiment et organisation criminelle, il dément avoir fait quoi que ce soit d'illégal et affirme n'avoir pas eu connaissance que sa messagerie était utilisée par des criminels.
L'entreprise. Les administrateurs de Sky Global développaient l'application et l'infrastructure informatique, activaient et désactivaient les cartes SIM selon les instructions des distributeurs et des revendeurs, avaient aussi la possibilité de supprimer à distance le contenu des appareils.
Les distributeurs. C'étaient des sociétés, souvent canadiennes, à charge pour elles de gérer le réseau de distributeurs, de recevoir le paiement des abonnements, d'apporter le cas échéant un support technique. Ils étaient liés à Sky Global par un accord-cadre.
Les revendeurs et les agents. Ces partenaires commerciaux achetaient des licences auprès des distributeurs, licences qu'ils revendaient ensuite en percevant une commission. Ils assistaient techniquement les utilisateurs. Plusieurs revendeurs belges – la plupart au nord du pays – ont été identifiés. JO.MA.

3.000.000

Trois millions d'échanges cryptés par jour.

4.439

4.439 suspects identifiés en Belgique.

600

600 dossiers judiciaires en Belgique.

1.000.000.000

Un milliard de communications interceptées.

La messagerie du crime

Une dizaine de médias*, dont *Le Soir*, ont mené l'enquête sur Sky ECC à partir des 3.800 documents issus du dossier judiciaire français : la justice française entend en effet déférer devant un procès d'assises des responsables de la société à l'origine de cette messagerie cryptée, ainsi que des distributeurs et revendeurs. Ces fichiers ont été recoupés et complétés par d'autres documents judiciaires et administratifs obtenus notamment en France, en Allemagne, aux Pays-Bas, en Belgique et en Serbie. Ainsi que par de nombreuses rencontres et interviews. JO.MA.

*L'enquête se base sur des documents obtenus par Studio-Fact (France), partagés et enrichis avec *Télérama* (France), Paper Trail Media et ZDF (Allemagne), RTBF, *Le Soir*, *De Standaard* (Belgique), *NRC* (Pays-Bas), CBC / Radio-Canada (Canada), Krik (Serbie), *Der Standard* (Autriche), Investigate.cz (République tchèque), Organized Crime and Corruption Reporting Project (OCCRP).

Réputée inviolable, l'application a cédé en 2021 sous les assauts répétés des polices belge, française et néerlandaise. © JAMES O'BRIEN (OCCRP).