ENQUÊTE

Sky ECC : les coulisses d'une opératio

Des milliers de documents inédits analysés par une dizaine de médias, dont « Le Soir », racontent la chute de Sky ECC, une messagerie ultrasécurisée avec laquelle les criminels partageaient leurs pires secrets. La police belge a largement contribué à cette opération d'infiltration.

Illustration réalisée par « Le Soir » sur base d'échanges réels tenus sur Sky ECC le 8 mars 2020.

JOËL MATRICHE

Cent quinze condamnations, 58 arrestations immédiates, des confiscations pour plusieurs dizaines de millions d'euros : il y a moins d'un mois, le tribunal correctionnel de Bruxelles sanctionnait sévèrement les membres d'organisations criminelles actives dans l'importation et la transformation de cocaïne. Un verdict long de 1.500 pages qui s'appuie en grande partie sur le piratage et le déchiffrement de la messagerie cryptée Sky ECC.

Réputée inviolable – son inventeur, le Canadien Jean-François Eap[1], avait promis une récompense de 5 millions de dollars à qui parviendrait à en briser les verrous –, l'application a pourtant cédé en 2021 sous les assauts répétés des polices belge, française et néerlandaise. Leur livrant un échantillon sans pareil du pire de la criminalité organisée : trafic de stupéfiants, bastonnades et tortures, meurtres et règlements de comptes… En janvier 2024, le succès de l'opération Sky ECC lancée trois ans plus tôt avait permis d'initier ou renforcer près de 600 dossiers judiciaires, d'identifier 4.439 suspects dans des affaires criminelles, de saisir l'équivalent de 180 millions d'euros. Les milliers de fichiers issus du dossier français – une cour d'assises devrait juger à Paris, probablement l'an prochain, des responsables de l'entreprise qui commercialisait Sky ECC ainsi que des revendeurs – auquel ont eu accès treize médias, dont *Le Soir*, jettent un éclairage nouveau sur cette traque sans précédent dans l'histoire du crime. Et de ceux qui le pourchassent.

Enlevé à la sortie d'une salle de fitness

A l'origine de ce thriller techno-judiciaire, Jean-François Eap, un entrepreneur de Vancouver qui, dès 2010, convaincu que la sécurité des téléphones portables est insuffisante, décide de créer avec un associé un produit qui renforce celle des BlackBerry. Vedettes du show-business, activistes des droits de l'homme, journalistes, avocats constituent alors le cœur de cible de la société Sky Secure (qui deviendra Sky Global) et de sa messagerie Sky ECC. « Nous avons mis au point une technologie qui rend le pouvoir aux utilisateurs », commente Jean-François Eap – il est inculpé en France et aux Etats-Unis. Si le rappeur Drake est réputé avoir possédé un de ces téléphones sécurisés – ce qu'il n'a pas souhaité commenter –, c'est au sein de la grande criminalité qu'ils ont suscité le plus vif enthousiasme.

En 2016, tandis que la start-up de Vancouver embauche des ingénieurs à tour de bras et investit de plus vastes bureaux, à 8.000 kilomètres de là, Younes, le jeune frère et complice présumé d'Othman El Ballouti – suspecté d'être un des grands trafiquants de drogue d'Europe –, est enlevé à la sortie d'une salle de sport anversoise par un commando. L'enquête démontrera que le téléphone portable utilisé par les ravisseurs est un BlackBerry. Intraçable car se connectant à un réseau privé : il s'avérera qu'il était équipé de Sky ECC. Intervenant pour une fusillade, pour un incendie criminel, le démantèlement d'un laboratoire de fabrication d'amphétamines ou des expéditions de cocaïne, les services de police belges ramassent encore, en 2016 et 2017, des dizaines de cryptophones impénétrables mais qu'ils n'auront de cesse, pendant cinq ans, de disséquer puis neutraliser.

En septembre 2018, un policier anversois résume dans un procès-verbal à l'attention de sa hiérarchie et du procureur du Roi les premiers résultats de ce qui n'est encore qu'une enquête menée localement. « Dans plusieurs enquêtes judiciaires confiées à la police judiciaire fédérale d'Anvers, des téléphones portables de type BlackBerry ont été présentés pour exploitation », écrit l'agent dans ce qui constitue, en quelque sorte, l'acte fondateur du dossier Sky ECC. « Un constat est que ces BlackBerry sont toujours équipés du logiciel de cryptage de la société Sky et également toujours équipés d'une carte SIM d'AT&T. »

Coffre-fort électronique

La protection de ces appareils est de niveau militaire, aucun policier n'est alors parvenu à en lire le contenu. Leur carte SIM n'autorise, par exemple, que le transfert de données, ce qui rend impossible leur localisation par l'envoi de SMS silencieux : cette technique consiste pour la police à envoyer des textos invisibles sur le téléphone des suspects, le portable ciblé renvoie alors une notification de réception à l'opérateur et par triangulation, l'appareil et son propriétaire peuvent théoriquement être localisés. Par sécurité aussi, le micro et la caméra sont inopérants lorsque le téléphone n'est pas en mode messagerie ; les messages sont automatiquement effacés après 48 heures si l'utilisateur ne les sauvegarde pas dans un coffre-fort électronique et, en cas d'urgence, l'encodage d'un mot de passe prédéfini provoque l'irréversible disparition de tout le contenu de l'appareil. Ce contenu peut aussi être supprimé à distance, par une tierce personne, voire par l'entreprise de Jean-François Eap – même si celui-ci se défend d'avoir jamais autorisé la neutralisation d'un smartphone qui avait été saisi par la police. Enfin, raffinement digne d'un film d'espionnage, l'application de messagerie peut être dissimulée sous la calculatrice : à l'utilisateur de lancer une opération mathématique bien précise pour activer Sky ECC.

Le prix de l'abonnement est à l'avenant – 200 euros par mois –, sans commune mesure avec ce que proposent les concurrents : Signal, WhatsApp et Telegram sont gratuits, la version la plus complète de Threema est facturée 3 euros par mois. Deux cents euros auxquels il faut ajouter l'achat d'un téléphone adapté puisque si l'application Sky ECC est initialement conçue pour les BlackBerry, elle sera ultérieurement déclinée pour les iPhone et les Google Pixel.

Nom de code, Froomie

Assez rapidement, avant même de partager leurs découvertes et leurs inquiétudes avec le parquet, les enquêteurs remarquent que quasiment rien n'est stocké dans la mémoire des téléphones, les clefs de cryptage, de même que la liste des contacts et la configuration de l'appareil sont stockés sur un serveur avec lequel le téléphone de l'utilisateur dialogue en passant par un réseau privé appelé APN (Access Point Name).

Un APN est une passerelle qui permet au téléphone mobile de se connecter à internet. Chez la plupart des fournisseurs, l'APN est public et dès qu'une carte SIM est insérée dans le téléphone, celui-ci s'y connecte automatiquement. L'APN de Proximus, par exemple, est internet.proximus.be et celui de Base est gprs.base.be. Mais certains groupes d'utilisateurs peuvent avoir un APN privé, qui crée une connexion sécurisée avec le réseau de l'entreprise. Sky ECC utilisait ainsi au moins cinq APN réservés.

Les demandes de connexion à un APN, quel qu'il soit, étant visibles par les opérateurs – SKY ECC ne travaillait qu'avec AT&T (USA), Movistar (Espagne) et KPN (Pays-Bas) –, il était par conséquent possible pour ceux-ci de connaître le nombre d'utilisateurs connectés à un instant t et, d'autre part, de les géolocaliser.

Ne travaillant qu'en sources ouvertes, les policiers relèvent aussi que toutes les communications cryptées transitent par les serveurs de l'entreprise française OVH et que ces serveurs sont loués par Sky Global, la société canadienne de Jean-François Eap.

Transmis d'abord aux autorités anversoises en septembre 2018, un PV initial de 31 pages est relayé aussitôt au parquet fédéral et, en novembre de l'année suivante, le dossier est mis à l'instruction – nom de code, Froomie – à Malines, chez le juge Philippe Van Linthout.

Surveillance massive

Parce qu'il s'avère que dans le même temps, les autorités néerlandaise et française investiguent, elles aussi, sur les usages potentiellement illégaux qui seraient faits de Sky ECC, une équipe d'enquête commune (ECE) est mise en place en décembre 2019 sous la supervision d'Europol. Trois magistrats et quinze enquêteurs belges en font partie. A ce moment, les juges de Lille ont déjà autorisé ce qu'un magistrat néerlandais avait refusé : intercepter, même si elles sont chiffrées, toutes les communications transitant par le centre d'OVH à Roubaix. Pour parvenir à cette surveillance massive et indiscriminée – il s'agissait de capter indistinctement tous les messages, sans que leur substance criminelle soit avérée –, le mandat autorise les enquêteurs à copier en temps réel toutes les données échangées entre le serveur principal que louait Sky Global et le serveur de sauvegarde. Au rythme affolant de trois millions d'échanges par jour, la nasse qu'avait lancée la justice se remplit rapidement. Et l'enquête transnationale enregistre de premiers résultats car si le contenu des messages demeure invisible, leurs métadonnées, autrement dit le contexte numérique de ces échanges, sont tout à fait lisibles : adresses IP des téléphones, identifiants alphanumériques de ces mêmes appareils et des cartes SIM, horodatage des conversations et des transmissions de fichiers (photos, messages vocaux), codes pin et surnoms des abonnés de Sky ECC, noms des groupes de discussion, etc.

Environ 70.000 codes pin, et donc a priori autant d'utilisateurs, sont actifs à ce moment, dont 10 % en Belgique. De ces 7.000 Belges, la plupart s'agitent dans la zone portuaire d'Anvers, malheureusement réputée pour ses transbordements fréquents de cocaïne. Même si c'est dans une moindre mesure, des grappes d'utilisateurs sont aussi détectées dans l'agglomération bruxelloise, à Charleroi et en région liégeoise, le long des grands axes routiers.

En analysant l'activité de ces cryptophones, notamment en croisant les voyages internationaux avec les listes de passagers d'avions et en consultant les enregistrements des caméras ANPR (qui enregistrement automatiquement les immatriculations) lors de déplacements domestiques, en recensant les antennes relais qui sont le plus sollicitées la nuit (ce qui peut donner une idée de l'endroit où dort l'utilisateur du téléphone), en fouillant dans les bases de données policières, les enquêteurs par-