Ransomwares : la France cède-t-elle « trop facilement » ?

La France, poule aux œufs d'or pour les opérateurs de *ransomwares* ? On en a débattu hier au Sénat, à l'occasion d'une table ronde sur la cybersécurité des ETI, PME et TPE.

Parmi les intervenants figurait **Johanna Brousse**. L'intéressée est vice-procureur au tribunal judiciaire de Paris. Elle dirige la section J3, dédiée à la lutte contre la cybercriminalité. Chiffres à l'appui, elle a peint un sombre tableau de la menace rançongiciel. Et soulevé, entre autres éléments, « une vraie question qui mérite toute [notre] attention » : celle du paiement des rançons.

« Aujourd'hui, la France est l'un des pays les plus attaqués […] parce que nous payons trop facilement », a déclaré la magistrate. Dans son collimateur, en particulier, les assureurs.
Guillaume Poupard se montre tout aussi dubitatif à leur propos. Certains jouent « un jeu trouble », affirme le directeur général de l'ANSSI. Non sans admettre qu'il en va de choix rationnels : il est tentant de payer quelques millions d'euros de rançon plutôt que des dizaines de millions d'euros de préjudice.

Ransomwares : les États-Unis, bon ou mauvais exemple ?

On est là dans un dilemme du prisonnier, où l'intérêt individuel est toujours de trahir, résume Guillaume Poupard. Bref, « on a un gros travail » pour enclencher une dynamique de résistance collective. Aux États-Unis, la Conférence des maires avait donné une impulsion dans ce sens à l'été 2019. L'organisation avait appelé les villes qu'elle représente – celles de plus de 30 000 habitants – à ne plus payer les rançons.

En France aussi, on mise sur l'exemplarité des acteurs publics. Parmi eux, les hôpitaux, cibles phares ces derniers mois. Pourquoi une telle recrudescence des attaques à leur encontre alors qu'ils ne peuvent pas payer ? s'est interrogé un membre de la DGE présent à la table ronde. On lui a donné la réponse suivante : les établissements de santé américains ont donné le mauvais exemple, en étant les premiers à payer. Les grandes municipalités ont fait de même jusqu'à l'accord sus-évoqué.

Quant aux assureurs, il faudra, reconnaît Guillaume Poupard, « faire la chasse à tous ces intermédiaires un petit peu gris […] qui vont se rémunérer parfois sur leur capacité à négocier, avec les criminels, l'abaissement des rançons ». Un comportement que le DG de l'ANSSI qualifie d'« extrêmement malsain ».

La J3 contre les silos

La section J3 fait partie de la Junalco (Juridiction nationale de lutte contre la cybercriminalité organisée), née l'an dernier. Chargée de se saisir des affaires les plus « emblématiques » dans ce

domaine, elle centralise les dossiers sur le plan national.

Une autre centralisation a été mise en place : celle des saisines en matière de *ransomwares*. La section J3 se saisit en l'occurrence de l'ensemble des dossiers sur le territoire national et co-saisit systématiquement la sous-direction de lutte contre la cybercriminalité (la police nationale, à Nanterre).

« On ne peut plus fonctionner en silos […] avec d'un côté le C3N qui va s'occuper de ses dossiers, le BL2C qui va s'occuper [des siens] et l'OCLCTIC qui va là encore travailler sur ses procédures », déclare à ce sujet Johanna Brousse. « Il faut créer des liens [car] aujourd'hui […], raisonner en termes de familles de *ransomwares*, c'est un non-sens, poursuit-elle. Vous avez des équipes interchangeables qui fonctionnent de manière transversale. […] Il est indispensable d'avoir une vue globale pour pouvoir cartographier la menace ». La démarche, assure-t-elle, a déjà porté ses fruits. Elle en veut pour preuve les opérations de démantèlement récemment menées contre Egregor et le *botnet* Emotet.

Cybercriminalité : au-delà des territoires

En l'état du droit demeure une difficulté : l'impossibilité, pour les services judiciaires, de communiquer officiellement des données à la DGSE et à l'ANSSI. Et *vice versa*. Une aberration, estime Johanna Brousse, quand on sait qu'aux États-Unis, les frontières sont bien plus poreuses entre l'appareil judiciaire et les services de renseignement. Aussi ces derniers peuvent-il avoir, dans le cadre des démarches de coopération internationale, connaissance d'informations que n'ont pas leurs homologues français. Le ministère de l'Intérieur porte actuellement une proposition de loi destinée à corriger le tir.

Autre complication : faire venir les cybercriminels en France pour les juger. Surtout lorsqu'ils se trouvent dans des pays qui ne collaborent pas.
Ce problème de « déterritorialisation » se retrouve dans la réaction aux attaques. De manière générale, on ne peut lancer un offensive sur des serveurs situés à l'étranger sans demander au préalable le concours des pays concernés.

Dans les cas les plus graves, la loi française permet de faire appel à des capacités offensives. Qui ne sont plus du domaine judiciaire, mais militaire. Par le biais du corpus existant, le Premier ministre peut aussi autoriser une démarche de « qualification » des menaces. C'est-à-dire la connexion à l'infrastructure d'attaque afin de « chercher à comprendre ce qui se passe », pour reprendre les termes de Guillaume Poupard.