Ce que WannaCry nous dit sur la régulation du chiffrement

Une démonstration par l'absurde ? C'est en tout cas la façon dont Tristan Nitot, le fondateur de Mozilla Europe aujourd'hui chef produit chez Cozy Cloud, interprète les récents ravages du ransomware WannaCry, qui a occupé la Une des médias internationaux le week-end dernier. Pour l'auteur de *Surveillance://*, l'épisode montre surtout l'incapacité des Etats, y compris ceux dotés de moyens considérables comme les Etats-Unis, à protéger leurs secrets. Car, avant de 'récupérer' un exploit développé par la NSA (EternalBlue), WannaCry n'était, dans sa première version, qu'un ransomware de plus à la capacité de nuisance limitée.

Le lien avec le chiffrement ? Pour Nitot, l'affaire montre le danger qui existe à mettre entre les mains d'autorités des secrets ou des armes numériques capables de saper la sécurité informatique globale. Or, c'est ce que réclament, selon lui, les gouvernements souhaitant affaiblir le chiffrement.

« L'industrie doit tenir bon »

« *Des gouvernements nous expliquent que le chiffrement fort est gênant dans l'exercice de leurs fonctions, et qu'il faudrait passer à un chiffrement à deux vitesses, pour lequel le gouvernement disposerait de clés spéciales*, écrit Tristan Nitot, sur le blog de Cozy Cloud. *Pour eux, en possession de telles clés, déchiffrer les communications serait facile, mais cela resterait presque impossible pour tout le reste du monde. Mais on l'a vu encore et encore, et WannaCry n'est qu'un exemple supplémentaire, les gouvernements n'arrivent pas à garder de tels secrets. Les clés spéciales finiront par fuiter, ce qui veut dire que le chiffrement fort deviendra d'un coup faible. La sécurité informatique ne sera plus qu'un bon souvenir.* »

De quoi saper la confiance dans toute les applications numériques. « *En d'autres mots, l'économie du monde s'arrêtera dans un grand fracas* », pronostique l'expert. Qui ajoute : « *En tant qu'industrie, nous devons tenir bon et refuser de dégrader la force du chiffrement, nous devons refuser les clés spéciales pour le gouvernement.* »

La charge anti-chiffrement de Macron

Le sujet risque de se retrouver très vite à l'agenda du nouveau gouvernement, l'Union européenne ayant prévu de présenter un projet de texte européen sur le sujet dès le mois de juin. Début avril, alors candidat, le président Macron avait accusé les « *grandes compagnies d'Internet* » d'abuser « *des facilités offertes par la cryptologie moderne* » et de refuser « *de communiquer leurs clefs de chiffrement ou de donner accès au contenu* » des communications. Plaidant pour une « *obligation (faite aux prestataires, NDLR) de livrer les codes* ».

Des déclarations qu'avaient du atténuer Mounir Majhoubi, alors directeur de la campagne numérique d'Emmanuel Macron et désormais secrétaire d'Etat au numérique. Dans un texte co-rédigé avec Didier Casas, ancien secrétaire général de Bouygues Telecom rallié à En Marche, le plus jeune ministre du gouvernement expliquait alors que l'objectif d'Emmanuel Macron n'était pas

« *d'obtenir la communication des clés de chiffrement utilisées par les prestataires* », mais plutôt mettre en place un système de réquisitions légales, les prestataires en question étant priés de fournir les données en clair. Un mécanisme sur lequel l'UE semble alignée, mais qui risque de se heurter aux services proposant un chiffrement de bout en bout. Et qui ne fait que déplacer la question de la protection des secrets soulevée par Tristan Nitot, des gouvernements aux entreprises.

A lire aussi :

Chiffrement : Emmanuel Macron marche en rond

Steve Kremer, Inria : « affaiblir le chiffrement, c'est grotesque »

L'Europe va proposer une législation affaiblissant le chiffrement