La mystérieuse "assurance" de Wikileaks

- Informatique - Internet -

Date de mise en ligne : jeudi 5 août 2010

Le fichier "pèse" 1,4 giga-octets, soit environ le quart d'un DVD. Il est compressé et crypté. Il s'appelle "assurance", et est apparu sur la page consacrée aux "journaux de guerre afghans" de Wikileaks, le 30 juillet. Et jusqu'ici, personne - en dehors des administrateurs du site - ne sait ce qu'il contient.

Lundi 26 juillet, Wikileaks, spécialisé dans la publication anonyme de documents secrets, avait rendu publics plus de 70 000 rapports de l'armée américaine en Afghanistan, un ensemble de documents baptisé "journaux de guerre afghans". Depuis, le Pentagone est à la recherche de l'informateur ayant transmis les documents au site, et de nombreuses voix se font entendre aux Etats-Unis pour réclamer des sanctions exemplaires contre le Wikileaks et sa ou ses sources.

Quelle est donc cette "assurance" publiée par le site ? Interrogé sur le contenu de cette archive, le porte-parole du site, Julian Assange, a expliqué qu'"il valait mieux qu'[il] ne fasse pas de commentaires sur ce fichier". Avant de titiller ses interlocuteurs : "On pourrait facilement imaginer une situation comme la nôtre, où il vaudrait mieux s'assurer que des documents historiques importants ne disparaissent pas."

CRYPTAGE INVIOLABLE

Les documents semblent avoir été chiffrés en utilisant l'Advanced encryption standard, un système de cryptage puissant - et utilisé par les agences gouvernementales américaines. Depuis 2005, c'est l'un des systèmes de cryptage utilisés par la très secrète National security agency (NSA). Conçu pour résister aux tentatives de décodage classiques, ce système ne peut a priori être cassé qu'en utilisant la "force brute", à savoir l'essai successif de toutes les combinaisons de caractères possibles. Un processus extrêmement long, qui nécessiterait des années de recherche avec des ordinateurs très puissants, notamment lorsqu'une clef de chiffrement longue est utilisée - ce qui serait le cas pour "l'assurance" de Wikileaks.

Face à ce fichier a priori inviolable, experts et curieux en sont réduits aux conjectures. L'"assurance" contient-elle l'intégralité des rapports afghans, y compris ceux que Wikileaks affirme ne pas avoir publiés pour protéger des informateurs de l'armée américaine ? Les télégrammes diplomatiques que Bradley Manning, le soldat inculpé pour avoir transmis une vidéo au site, est soupçonné d'avoir également dérobé ? Ou bien s'agit-il d'un bluff, et d'un fichier vide ? La taille importante du fichier laisse entendre qu'il pourrait s'agir soit d'une vidéo soit d'une très grande quantité de fichiers texte. Des utilisateurs du forum abovetopsecrets ont fait le calcul : si Wikileaks a bien en sa possession 260 000 télégrammes diplomatiques, l'ensemble des documents "pèserait" environ 1,7 giga-octets.

En rendant public le fichier, Wikileaks s'est de toute manière assuré que de multiples copies en seraient effectuées dans tous les pays du monde. Si le site dévoile la clef de décryptage, il s'assure que les documents resteront publics, même en cas de fermeture de Wikileaks. La clef pourrait avoir été d'ores et déjà transmises aux autorités américaines, estime le spécialiste de la sécurité Bruce Schneier, pour les dissuader de s'en prendre à Wikileaks. A condition, bien sûr, qu'il ne s'agisse pas d'un bluff.

Post-scriptum :

http://www.lemonde.fr/technologies/...