Réseaux sociaux, messageries, jeu vidéo… Comment les terroristes communiquent ?

Réseaux sociaux, messageries, jeu vidéo… Comment les terroristes communiquent ?

Les jihadistes utilisent abondamment les outils numériques de communication. Problème : ceux-ci sont de plus en plus difficiles à surveiller.

Les terroristes islamistes utilisent depuis toujours les outils numériques de communication qui présentent l'avantage d'être simples pour des personnes n'ayant pas de compétences particulières tout en étant terriblement puissants :
• Les réseaux sociaux pour la propagande publique (Youtube, Facebook, Twitter, etc.
• Les applis de messagerie et de voix sur IP pour la communication interpersonnelle (WhatsApp, Snapchat, Skype, iMessage, Viber, Telegram, etc.)

Même le jeu vidéo

Les terroristes utiliseraient même le jeu vidéo. C'est une information livrée avant les attentats de Paris par le ministre de l'Intérieur belge. Selon lui, la Playstation 4 serait exploitée pour communiquer vocalement via l'appli de voix sur IP intégrée au réseau PSN (PlayStation Network).
D'après Jan Jambon, ces communications seraient « plus difficiles à écouter que WhatsApp ». Les terroristes pourraient aussi faire passer de courts messages à des complices via les jeux eux-mêmes, par exemple : en « écrivant » sur un mur à l'aide de rafales d'armes au sein d'un jeu de tir (FPS). Ces messages sont quasiment indétectables et disparaîssent rapidement.
En ce qui concerne l'enquête sur les attentats de Paris, Une Playstation 4 a été saisie lors des perquisitions en Belgique. Cependant, rien de prouve, à cette heure, que celle-ci ait pu effectivement être utilisée par les auteurs de la manière décrite ci-dessus.

Chiffrement et porte dérobée

D'une manière générale, l'utilisation des outils numériques de communication pose des difficultés techniques et juridiques aux autorités chargées de la surveillance. Depuis l'affaire Snowden et les excès de surveillance de la NSA, les entreprises du secteur (Apple, WhatsApp, etc.) ont renforcé la sécurité de leurs outils pour rassurer leurs clients quant à la confidentialité des données personnelles.
Par exemple, la nouvelle version du logiciel iOS9 pour iPhone et iPad comporte désormais un code de déverrouillage à 6 chiffres au lieu de 4 plus difficile à craquer, y compris la firme Apple elle-même.
De son côté, WhatsApp chiffre les échanges de bout en bout ce qui garantit une totale confidentialité. C'est comme un coffre fort dont on aurait jeté la clé au fond d'un puits…
Dans le cadre de la lutte anti-terroriste, les Etats réclament la possibilité de pouvoir accéder aux communications numériques en bénéficiant des clés de (dé)chiffrement ou via des portes dérobées (backdoors) prévues à l'avance. Mais ces demandes sont en contradiction avec l'exigence de confidentialité des plus farouches partisans de la protection de la vie privée.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !
S o u r c e :
http://www.franceinfo.fr/emission/nouveau-monde/2015-2016/reseaux-sociaux-messageries-jeu-video-comment-les-terroristes-communiquent-16-11-2015-08-49