Silk Road : quand la fermeture du site star de l'Internet du crime bénéficie à des recoins encore plus sombres du web

Il n'y a pas que des armes ou des substances illicites qui peuvent s'acheter dans les "zones d'ombres" d'internet, il existe aussi des données identitaires ou bancaires qui se revendent à prix d'or.

Avec Michel Nesterenko

Atlantico : Depuis la fermeture du réseau "Silk Road" (NDLR, la route de la soie en anglais), de nouvelles plateformes proposant des produits illicites connaissent un nouvel essor sur le marché noir du web. En plus des armes et des stupéfiants, ce sont désormais des informations identitaire ou bancaires qui sont vendus à prix d'or. Comment l'expliquez-vous ?

Michel Nesterenko : Le marché des informations identitaires des citoyens, qui inclue les dossiers médicaux en plus des données financières et autres, a subit un essor phénoménal, depuis 1990, en suivant le développement d'internet. **La NSA, organe du gouvernement américain, à favorisé les cyber-criminels en installant et en cachant un très grand nombre de vulnérabilités, dans un but d'espionnage planétaire**.

Il s'agit aujourd'hui, en ce qui concerne l'activité criminelle à elle seule, d'un des plus grand marché commercial globalisé. Il s'agit de plusieurs dizaines de milliards annuels. Dès qu'il y a des acheteurs, il y a des des fournisseurs et internet est un parfait système de communication planétaire. Dans ce commerce il y a deux phases qui chacune nécessitent l'utilisation d'internet. La phase de collecte ou plutôt de vol. Et la phase de revente.

Il faut noter que même des sociétés cotées en Bourse participent à cette activité en vendant les informations privées de leurs clients sans autorisation. Google et autres géants du commerce électronique sont en ce moment ciblé par la Commission Européenne pour un commerce qui violerait les Lois Européennes.

Comment expliquer que les achats de produits illégaux prolifèrent sur internet, dans la deep zone, alors même que le système bancaire international devrait pouvoir interdire les fraudes ?

Même les services de police les plus performants du monde n'ont pas pu éradiquer le crime organisé, ni le trafic de drogue, pour ne citer que celui dernier. Lorsqu'il s'agit de petites sommes en jeu, le trafic est pratiquement indétectable, car les autorités de contrôle concentrent leurs maigres moyens sur les gros poissons et les grands trafics qui sont par nature plus visibles. Si on fait fermer un site

dix autres le remplacent instantanément, il suffit de voire la prolifération des sites jihadistes.

Les Banques n'ont jamais eu pour mission d'espionner les activités de tous leurs clients, bien que les autorités fiscales aujourd'hui cherchent à les enrôler pour faire une chasse active aux fraudeurs. Si par malheur, les Banques étaient forcées de devenir des auxiliaires de la police et du fisc, alors il faudra s'attendre à une explosion des frais bancaires pour tout le monde et un net ralentissement d'une grande partie du commerce national et international. Le résultat sera une crise économique et une explosion du chômage, sans pour cela gêner d'aucune façon les commerces illégaux qui se contenteront de changer de forme. Les nouvelles réglementations bancaires, instituées pour limiter les fraudes, et leurs effets secondaires extrêmement négatifs sur les économies des différents pays, sont un exemple de ce qui pourrait bien arriver à plus grande échelle.

Quelles sont les difficultés rencontrées par les services de police pour lutter contre la cybercriminalité dans la "deep zone" ? Comment se fait-il que ces plateformes de revente illégales ne tombent pas sous le coup de la loi ?

Les services de police manquent cruellement de moyens et de personnel formé pour traquer et capturer les nouveaux criminels agissant dans l'univers dématérialisé d'internet. **Les Lois elles mêmes doivent être adaptées avec les avancées rapides de la technologie et là c'est notre gouvernement et nos élus qui manquent de connaissance des enjeux.** Puis il est impératif de développer la coopération policière internationale car les cybercriminels se jouent des frontières qu'ils utilisent comme boucliers. Enfin il faut mettre en oeuvre au niveau des Nations Unies un système de sanctions rapides pour mettre au pas les pays qui protègent les cyber-criminels et hébergent les réseaux informatiques du crime organisé.

Le fait que ces échanges se déroulent dans la "deep zone" d'internet provoque-t-il de nouveaux obstacles ?

Il s'agit moins d'obstacles que d'un accroissement des coûts. La "deep zone" d'internet ne freine en aucun cas l'espionnage de la NSA avec ses moyens illimités. Il ne faut pas oublier toutes les données cryptées qui exigent des super ordinateurs fort coûteux pour craquer les codes. Moyenne en quoi la deep zone est un lieu de pêche très très riche pour les espions et les criminels ainsi que pour les entreprises, les industriels et la recherche scientifique.

Propos reccueillis par Sarah Pinard