Passer la douane avec un ordinateur portable

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 5 juin 2009

Spyworld Actu

... 1er épisode : La Chine

Lors de mes voyages à l'étranger je me suis fait contrôler à plusieurs reprises mon ordinateur portable à la douane ; Hasard ? Nécessité ? Pourquoi les douaniers contrôlent-ils de plus en plus les ordinateurs qui rentrent dans leur pays et comment réagir ?

« Shanghai 8h50 - poste de douane de l'aéroport de Pudong »

- Can I see your laptop sir ?
- Yes certainly
- We need to proceed to a deep investigation, this is a routine control. Can you wait in this room for 15 minutes ?
- Sure I wait (le douanier n'a pas encore tamponné le visa d'entrée) 25 minutes plus tard, le douanier revient, embarrassé :
- Can you unlock your computer Sir ?
- Sure (si vous refusez vous risquez de ne pas rentrer dans le pays, je n'ai pas essayé...)
- Je glisse le doigt sur le lecteur biométrique et le douanier repart avec mon PC satisfait... Quelques minutes plus tard il revient, radieux :
- No problem Sir you can proceed...

Démarrage du PC avec une clé USB Linux

Que s'est-il passé en coulisse ? Le douanier a démarré le portable avec une clef USB contenant une version de Linux de type Ubuntu, qui permet d'éviter le boot Windows, et donc le mot de passe qui va avec. Il visualise ensuite tous les fichiers dans « Mes documents » et les copie sur la clef USB. Il éteint ensuite le PC et vous le restitue. Variante : Il « ghoste » tout le disque dur, ce qui prend un peu plus longtemps, de l'ordre de 20 minutes pour 60 Go. L'avantage de faire une copie de tout le disque est de trouver des documents dans le cache Windows, ou bien des mots de passe ou des cookies, ainsi que l'historique de tous les sites explorés par l'utilisateur.

Pourquoi le douanier m'a-t-il demandé de déverrouiller mon ordinateur ? Parce qu'il n'a pas pu booter la clef USB avec Linux et n'a pas pu accéder au disque dur, celui-ci étant chiffré et protégé par biométrie. J'avais deux options : soit refuser de déverrouiller le portable auquel cas j'aurais pu être refoulé, ou arrêté, soit accepter et donner accès à mon disque. Ont-ils récupéré des informations sensibles, comme des audits sécurité de clients, ou bien d'autres informations économiquement intéressantes ?

Quelle parade ?

La réponse au passage de douane en Chine est double : soit vous chiffrez le disque dur, avec la possibilité de vous faire refouler, si les autorités n'ont pas accès au disque (c'est le cas dans de nombreux pays pour lutter contre le terrorisme et les fraudes financières), soit vous arrivez avec un ordinateur « vide », et vous vous connectez en extranet en utilisant un canal chiffré (SSL). Ainsi, la plupart des consultants internationaux et avocats préconisent de passer toute douane avec un ordinateur ne contenant aucun fichier sensible, et de se connecter à distance à leur bureau ou à un dispositif de type « Google docs » et Gmail.

Un utilitaire comme Truecrypt

Bruce Schneier, grand guru de la sécurité, préconise l'utilisation de la stéganographie, notamment en créant une partition chiffrée cachée sur le disque à l'aide d'un utilitaire dédié comme Truecrypt. C'est une bonne idée, mais si la

douane se rend compte de la tactique, il se peut que les ennuis soient bien pires que le remède.

Post-scriptum :

http://www.01net.com/editorial/5030...